РЕАЛИЗАЦИЯ РЕГИСТРАЦИИ И АУТЕНТИФИКАЦИИ В РАЗРАБОТКЕ ПРИЛОЖЕНИЙ

Иманов В. А., студент 3 курса физико-математического факультета по направлению «Прикладная информатика в информационной сфере»

г. Бирск, ФГБОУ ВО «Уфимский университет науки и технологий»
Бирскийфилиал УУНиТ

Введение

В настоящее время все больше разрабатываются многопользовательские приложения для общего пользования. Соответственно, регистрация и авторизация пользователей является особенно важной частью при разработке таких приложений. Регистрация позволяет создавать пользователям учетные записи с их персональными данными.

В свою очередь, аутентификация позволяет определить конкретного пользователя, вошедшего в систему[4].

Методы реализации регистрации

Существует несколько методов реализации регистрации

- Регистрация по e-mail;
- Регистрация с использованием социальных сетей.

Метод регистрации по e-mail

Если рассматривать регистрацию по e-mail, то его механизм представлен следующим образом.

Клиентская часть приложения имеет некоторую форму регистрации, которая предоставляет возможность ввода персональной информации пользователя. Обычно это поля для логина, пароля, имени, фамилии, а также электронной почты.

Рисунок 1. Пример формы регистрации

В серверной части же используются базы данных для хранения информации.

Важной частью при регистрации является проверка информации, введенной пользователем на действительность (валидация данных), а также на наличие таких же данных в базе данных приложения.

До завершения регистрации, у пользователя будет активна временная учетная запись. Временная учетная запись не имеет доступа к основным функциям приложения и необходима лишь для того, чтобы создать новую учетную запись и пройти регистрацию. Это позволит организовать гибкую систему прав доступа в приложении.[1]

Завершением регистрации является подтверждение пользователем адреса электронной почты и отправки формы с клиентской части на сервер. [1]

Метод регистрации через социальные сети

Регистрация через социальные сети предполагает использование определенных API, которые предоставляют персональные данные, с разрешения пользователя. При этом, схема регистрации использует те же самые механизмы, что и при регистрации с использованием электронной почты – это проверка действительности и уникальности данных.

Процесс аутентификации

Процесс аутентификации предполагает проверку подлинности пользователя, а также разрешения доступа к некоторым ресурсам. Механизм заключается в проверке сервером данных, введенных пользователем и данных, хранящихся в базе данных и не только.[4]

Методы аутентификации

Существует множество способов аутентификации:

- Аутентификация по паролю (обычное сопоставление комбинации символов);

– Аутентификация на основе биометрических данных пользователя (отпечатки пальцев, рисунок радужной оболочки глаза, данные лица, и пр.);

– Аутентификация с помощью SMS (отправка специального ключа в виде текстового сообщения на номер телефона);

– Аутентификация через географическое положение (проверка подлинности удаленного пользователя по его местоположению);

– Аутентификация с помощью токенов.[4]

Токены аутентификации

Токены являются распространенным методом аутентификации в современных приложениях. Аутентификация с помощью токенов подразумевает получение пользователями сгенерированный код (токен), который предоставляет дальнейший доступ к системе. Обычно аутентификация с помощью токенов используется совместно с аутентификациейпо паролю для обеспечения большего уровня безопасности.[2]

JWT (JSONWebToken)

Одним из известных токенов является JWT-токен (открытый стандарт (RFC 7519)). JWT использует объекты JSONдля передачи.JWTимеет небольшой размер, но при этом содержит всю необходимую информации о пользователе, что позволяет сократить многократное обращение к базам данных.

В своей компактной форме веб-токены JSON состоят из трех частей, разделенных точками: заголовок, полезная нагрузка, подпись. Поэтому JWT выглядит обычно выглядит следующим образом: «xxxx.yyyy.zzzz».[3]

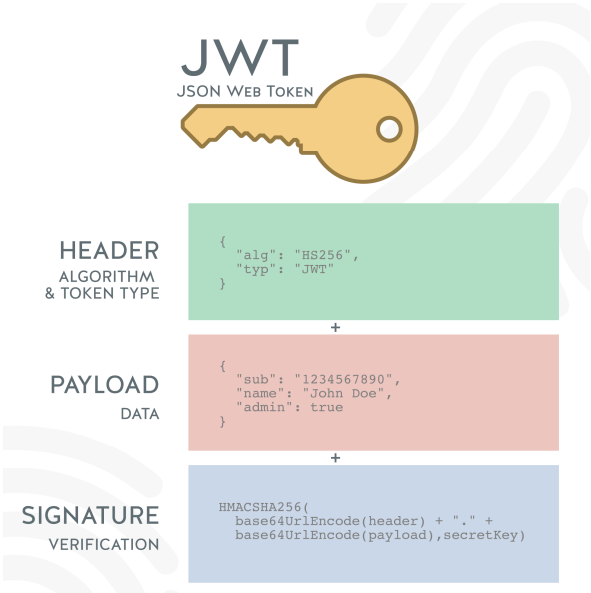

Рисунок 2. Структура JWT

Вывод

В данной статье были рассмотрены общие механизмы, методы регистрации и аутентификации пользователей, использующихся при разработке современных приложений.

Для описания теоретической части были использованы следующие источники информации– [1, 2, 3, 4]

Библиографический список

1. Павел Шерер. Инструкция: как написать идеальную регистрацию // vc.ru – Разработка [Электронный ресурс]. URL: https://vc.ru/dev/156552-instrukciya-kak-napisat-idealnuyu-registraciyu (дата обращения 13.03.2023)
2. Токен авторизации // Habr[Электронный ресурс]. URL: https://habr.com/ru/post/534092/ (дата обращения 13.03.2023)
3. Обзор аутентификации на основе токенов// Habr[Электронный ресурс]. URL: https://habr.com/ru/post/593191/(дата обращения 13.03.2023)
4. Аутентификация // Википедия [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/%D0%90%D1%83%D1%82%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D1%8F(дата обращения 13.03.2023)