

ПРОЕКТИРОВАНИЕ БЕЗОПАСНОЙ СИСТЕМЫ АВТОРИЗАЦИИ ДЛЯ ПРИЛОЖЕНИЯ ПО ПРОГНОЗИРОВАНИЮ ВЕРОЯТНОСТИ НАСТУПЛЕНИЯ РАЗЛИЧНЫХ СОБЫТИЙ

К.Р. Сварян, Н.Ю. Юдина

ФГБОУ ВО «Воронежский государственный лесотехнический университет
имени Г.Ф. Морозова»

Аннотация. В данной статье рассматриваются основные подходы и методы проектирования безопасной системы авторизации для приложений, связанных с обработкой и анализом чувствительной информации. Основное внимание уделено проектированию безопасной системы авторизации на основе JWT для приложения, предсказывающего вероятность наступления различных событий. Рассматриваются принципы работы JWT, их преимущества и уязвимости, а также приводятся рекомендации по их безопасной интеграции в систему. Обсуждаются методы защиты токенов от подделки, ротации ключей, использование криптографических алгоритмов и внедрение многофакторной аутентификации для повышения уровня безопасности.

Ключевые слова: безопасность данных, система авторизации, JSON Web Token (JWT), прогнозирование событий, защита данных, криптография, кибербезопасность, токены доступа.

DESIGNING A SECURE AUTHORIZATION SYSTEM FOR AN EVENT PROBABILITY PREDICTION APPLICATION

K.R. Svarian¹, N.Yu. Yudina¹

¹Voronezh State University of Forestry and Technologies named after G.F. Morozov

Abstract. This article examines the main approaches and methods for designing a secure authorization system for applications that involve the processing and analysis of sensitive information. The primary focus is on designing a secure authorization system based on JWT for an application that predicts the likelihood of various events. The principles of JWT operation, its advantages and vulnerabilities, as well as recommendations for its secure integration into the system, are discussed. Methods for protecting tokens from forgery, key rotation, the use of cryptographic algorithms, and the implementation of multi-factor authentication to enhance security are also considered.

Keywords: data security, authorization system, JSON Web Token (JWT), event prediction, data protection, cryptography, cybersecurity, access tokens.

В современных условиях быстрого увеличения объемов информации и высокой сложности информационных систем важной задачей становится

повышение уровня их безопасности. Особо актуальна эта задача для программных продуктов, которые предназначены для решения задач прогнозирования. Информационные системы прогнозирования работают с особо чувствительными данными, связанными с анализом рисков, экономическими прогнозами и другими, которые получены из важных сфер. Несанкционный доступ к таким информационным системам приводит к серьезным последствиям, например, потере данных, компрометации конфиденциальной информации и финансовым потерям.

Ключевым моментом в сфере обеспечения безопасности информационных систем является защита доступа к ним. Это как правило, обеспечивается системой авторизации пользователя. Применяемые методы авторизации учитывают такие факторы как потребность в масштабировании, распределенная архитектура, высокая нагрузка. В настоящее время JSON Web Token, благодаря своей гибкости и безопасности, стал наиболее востребован. JSON Web Token – это стандарт для обмена данными в web-приложениях. Он позволяет работать в распределенных системах.

JSON Web Token включает три основные части: заголовок (Header), полезная нагрузка (Payload) и подпись (Signature). Заголовок включает два поля – тип токена и алгоритм шифрования. Алгоритм шифрования используется для подписи токена. Тип токена всегда JWT. Формат кодирования Base64URL.

Полезная нагрузка содержит утверждения о пользователе, которые могут быть зарегистрированными, публичными или приватными. Она также кодируется в формате Base64URL.

Подпись содержит закодированный заголовок и полезную нагрузку, которые соединяются с секретным ключом и алгоритмом шифрования, указанным в заголовке. Такой метод позволяет быть уверенным в том, что токен реальный, а не подделка.

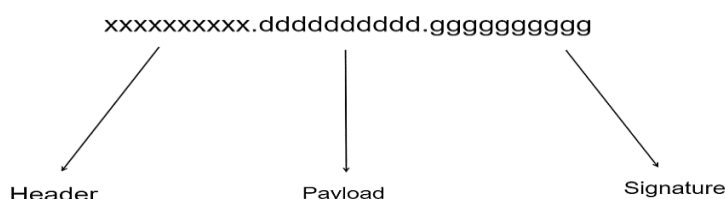


Рисунок 1 – Формат JSON Web Token токена

В процессе работы с JSON Web Token требуется выполнить аутентификацию пользователя, когда он вводит свои учетные данные и отправляет их на сервер. Если введенные данные верны, то генерируется JWT. Далее это JWT отправляется на компьютер клиента и там хранится.

При следующем входе клиент включает JWT в заголовок Authorization, используя схему "Bearer". На сервере происходит проверка токена путем сравнения его с токеном, который хранится на сервере. Если результат положительный, то пользователю будет предоставлен доступ к ресурсам. Токен проверяется также на подлинность подписи, истечения срока его действия. При

необходимости можно реализовать механизмы обновления токена, чтобы продлить сессию без повторного ввода учетных данных.

Благодаря этому JWT предлагает ряд преимуществ для систем авторизации, включая компактность, которая упрощает передачу токенов через сети, и независимость от состояния сервера, что устраняет необходимость в хранении сессионных данных и упрощает масштабирование приложений. Его высокая производительность обусловлена тем, что проверка токена выполняется непосредственно на сервере без обращения к базе данных. Эти характеристики делают JWT идеальным выбором для приложений, прогнозирующих вероятность событий, где важны безопасность и эффективность.

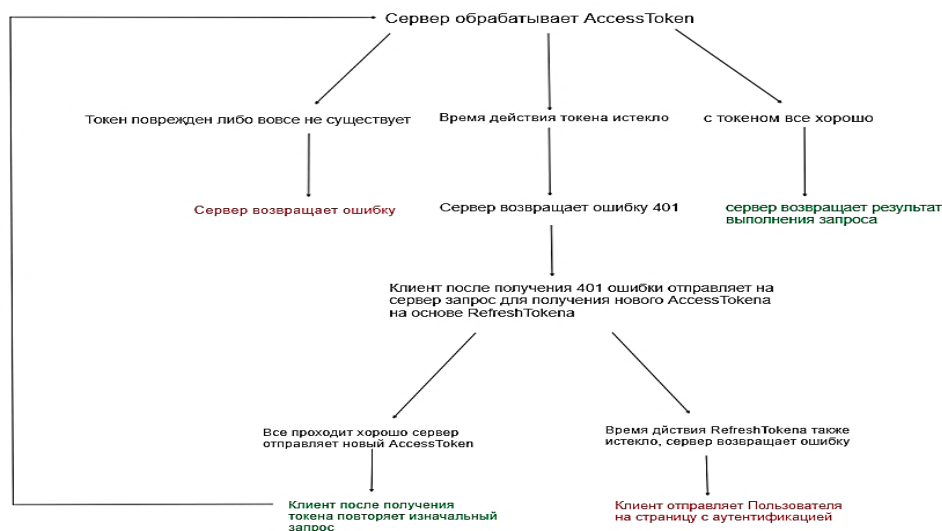


Рисунок 2 – Логика работы приложения

Проектирование безопасной системы авторизации для приложения по прогнозированию вероятности наступления различных событий является критически важной задачей, учитывая высокую ценность и чувствительность данных, с которыми работают такие системы. Использование JSON Web Token (JWT) в качестве основного механизма авторизации предоставляет мощный инструмент, обеспечивающий безопасность, гибкость и производительность системы.

Список литературы

1. Официальный сайт технологии JWT. – URL: <https://jwt.io/>.
2. RFC 7519. JSON Web Token (JWT). – URL: <https://tools.ietf.org/html/rfc7519>.
3. Рихтер, Дж. CLR via C#. Программирование на платформе Microsoft .NET Framework 4.5 на языке C# / Дж. Рихтер. – СПб.: Питер, 2019. – 896 с.
4. Бедердинова, О. И. Программирование на языках высокого уровня : учеб. пособие / О. И. Бедердинова, Т. А. Минеева, Ю. А. Водовозова. – Москва : ИНФРА-М, 2019. – 159 с. – URL: <https://znanium.com/catalog/product/1044396>. – Режим доступа: по подписке.

5. Lerman, J. Programming Entity Framework: Code First/ J. Lerman, R. Miller; O'Reilly Media, Inc, 2011. – 177 p. – ISBN 978-1449312947.

References

1. Official JWT Technology Website. – URL: <https://jwt.io/>.
2. RFC 7519. JSON Web Token (JWT). – URL: <https://tools.ietf.org/html/rfc7519>.
3. Richter, J. CLR via C#. Programming on the Microsoft .NET Framework 4.5 in C# / J. Richter. – St. Petersburg: Piter, 2019. – 896 p.
4. Bederdinova, O. I. Programming in high-level languages: textbook / O. I. Bederdinova, T. A. Mineeva, Yu. A. Vodovozova. – Moscow: INFRA-M, 2019. – 159 p. – URL: <https://znanium.com/catalog/product/1044396>. – Access mode: by subscription.
5. Lerman J., Miller R. Programming Entity Framework: Code First. – O'Reilly Media, Inc, 2011. – 177 p. – ISBN 978-1449312947.