УДК 004.056.55

Студ. Е.Д. Янукович
Науч. рук. ассист. Д.В. Сазонова
(кафедра информационных систем и технологий, БГТУ)

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПРОТОКОЛОВ АУТЕНТИФИКАЦИИ: JWT, OAUTH, SAML

Современные веб-приложения и цифровые сервисы предъявляют высокие требования к обеспечению безопасности пользовательских данных. Одним из важнейших компонентов информационной безопасности является аутентификация – процесс проверки подлинности пользователя перед предоставлением доступа к системе. Развитие технологий привело к появлению множества протоколов аутентификации, среди которых наибольшее распространение получили JWT, OAuth 2.0 и SAML. Каждый из этих протоколов решает задачи идентификации и авторизации по-своему, в зависимости от архитектуры, масштаба и назначения информационной системы.

JWT (JSON Web Token) – это открытый стандарт (RFC 7519), предназначенный для безопасной передачи информации между участниками в виде JSON-объекта. Токен состоит из трёх частей: заголовка, полезной нагрузки и криптографической подписи. Одним из ключевых преимуществ JWT является автономность: после аутентификации пользователя сервер возвращает токен, который может использоваться без повторных запросов к серверу. Это снижает нагрузку на сервер и повышает скорость отклика системы. Однако при использовании JWT необходимо уделять внимание безопасности токенов – например, предотвращению их кражи (token hijacking) и повторного использования.

OAuth 2.0 – это протокол авторизации, предназначенный для делегирования доступа к защищённым ресурсам без необходимости раскрытия учётных данных пользователя. В архитектуре OAuth участвуют сервер авторизации, клиент и ресурсный сервер. Клиент получает ограниченные токены доступа (access tokens) и, при необходимости, токены обновления (refresh tokens). Протокол поддерживает разные сценарии аутентификации, включая Authorization Code Flow, Implicit Flow, Client Credentials Flow и Resource Owner Password Credentials Flow. Одним из главных достоинств OAuth является его универсальность и активное применение в экосистемах крупных компаний: Google, Facebook, GitHub, Microsoft и других.

SAML (Security Assertion Markup Language) представляет собой XML-ориентированный стандарт для обмена данными об аутентифика-

ции и авторизации между доверенными доменами. Основными участниками являются провайдер идентификации (IdP) и провайдер услуг (SP). Одной из ключевых возможностей SAML является поддержка технологии SSO (Single Sign-On), позволяющей пользователю получать доступ ко множеству сервисов после однократной аутентификации. SAML широко используется в корпоративной среде, в том числе в Active Directory Federation Services, а также в образовательных и государственных учреждениях. Недостатками протокола являются сложность настройки и громоздкость XML-формата.

Сравнительный анализ протоколов показывает, что выбор конкретного решения зависит от условий проекта. JWT отлично подходит для современных веб-приложений с REST API и SPA-архитектурой (Single Page Applications), особенно в связке с OAuth 2.0. OAuth обеспечивает делегированную авторизацию и гибкость в интеграции с внешними сервисами. SAML оптимален для крупных организаций с централизованной политикой управления доступом.

Таким образом, каждый из рассмотренных протоколов имеет свои сильные и слабые стороны. JWT обеспечивает лёгкость и масштабируемость, OAuth – гибкость и безопасность при работе с третьими сторонами, SAML – централизованное управление и единый вход. Правильный выбор протокола аутентификации должен основываться на анализе требований безопасности, архитектуры системы и характера пользовательского взаимодействия.

ЛИТЕРАТУРА

1. Протоколы аутентификации [Электронный ресурс]. Режим доступа: https://habr.com/ru/companies/dataart/articles/262817/. Дата доступа: 03.04.2025

2. Протоколы авторизации [Электронный ресурс]. Режим доступа: https://habr.com/ru/sandbox/225864/. Дата доступа: 04.04.2025

УДК 004.056.55

Студ. В.А. Метрик, С.А. Валько
Науч. рук. ассист. Д. В. Сазонова
(кафедра информационных систем и технологий, БГТУ)

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ШИФРОВАЛЬНЫХ МАШИН: ХЕБЕРНА, М-209, ЭНИГМА, ЛОРЕНЦА

Шифровальная машина Эдварда Хеберна стала первой, где применялся роторный механизм. При нажатии клавиши электрический сигнал проходил через систему роторов с фиксированной внутренней проводкой, изменяя маршрут сигнала и шифруя символ. М-209 – пор-