Перевертун Д.Р. Методы аутентификации и управления доступом
// Международный журнал информационных технологий и энергоэффективности. - 2024. – Т. 9 № 5(43) с. 77–84

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.05

МЕТОДЫ АУТЕНТИФИКАЦИИ И УПРАВЛЕНИЯ ДОСТУПОМ

Перевертун Д.Р.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: danilaperevertun@gmail.com

В эпоху быстрого развития цифровых технологий и увеличения объемов конфиденциальной информации, хранящейся в электронном виде, вопросы аутентификации и управления доступом приобретают критическую важность. Статья охватывает широкий спектр методов и подходов к аутентификации и управлению доступом, включая традиционные пароли, биометрическую аутентификацию, многофакторную аутентификацию, адаптивную аутентификацию, а также применение децентрализованных идентификаторов и блокчейн технологий. Анализируя каждый из этих методов, статья выявляет их преимущества и недостатки, а также рассматривает потенциальные направления развития в области управления доступом и аутентификации для обеспечения высокого уровня безопасности в цифровом мире.

Ключевые слова: Аутентификация, управление доступом, многофакторная аутентификация, биометрическая аутентификация, децентрализованные идентификаторы, блокчейн, безопасность данных, цифровая идентичность, принцип наименьших привилегий, адаптивная аутентификация.

AUTHENTICATION AND ACCESS CONTROL METHODS

Perevertun D.R.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: danilaperevertun@gmail.com

In an era of rapid development of digital technologies and an increase in the volume of confidential information stored electronically, authentication and access control issues are becoming critically important. The article covers a wide range of methods and approaches to authentication and access control, including traditional passwords, biometric authentication, multi-factor authentication, adaptive authentication, as well as the use of decentralized identifiers and blockchain technologies. Analyzing each of these methods, the article identifies their advantages and disadvantages, as well as considers potential development directions in the field of access control and authentication to ensure a high level of security in the digital world.

Keywords: Authentication, access control, multifactor authentication, biometric authentication, decentralized identifiers, blockchain, data security, digital identity, principle of least privilege, adaptive authentication.

В современном мире, где информационные технологии играют ключевую роль в бизнесе, науке и повседневной жизни, вопросы аутентификации и управления доступом становятся все более актуальными. С развитием интернета вещей, облачных вычислений и мобильных технологий, необходимость в надежных методах проверки подлинности и управления доступом к ресурсам никогда не была более острой. Эта статья рассматривает

различные аспекты аутентификации и управления доступом, анализируя современные методы и подходы, их преимущества и недостатки, а также потенциальные направления развития в этой области.

Аутентификация — это процесс верификации идентичности пользователя, при котором система убеждается в том, что пользователь действительно является тем, за кого себя выдает. Управление доступом, в свою очередь, — это процесс, который после аутентификации определяет, к каким ресурсам и операциям пользователь имеет доступ. Эти два процесса тесно связаны, поскольку надежная аутентификация является основой для эффективного управления доступом.

В основе процессов аутентификации и управления доступом лежит идея верификации идентичности пользователя и последующего определения его прав на выполнение определенных действий или доступ к ресурсам. Эти процессы тесно связаны и играют важную роль в обеспечении безопасности информационных систем. Аутентификация представляет собой первый шаг, в ходе которого система должна убедиться, что пользователь или система действительно являются теми, за кого себя выдают.[6] Этот процесс можно сравнить с предъявлением документа, удостоверяющего личность, при входе в защищенное здание. Как только идентичность подтверждена, наступает этап управления доступом, который определяет, какие действия или ресурсы доступны пользователю на основе его прав и ролей в системе.

Этот механизм не просто черно-белый фильтр, пропускающий внутрь всех, кто успешно прошел аутентификацию; он более тонко настраивает уровень доступа каждого пользователя, гарантируя, что каждый имеет доступ только к тем ресурсам, которые необходимы для выполнения своих задач.[3] Так, например, сотрудник службы поддержки может иметь доступ к базе данных обращений пользователей, но не к финансовой информации компании, в то время как у бухгалтера будут права на просмотр и редактирование финансовых документов, но не обращений клиентов.

Важность такого подхода сложно переоценить, поскольку он лежит в основе защиты конфиденциальности и интегритета данных, а также обеспечивает соблюдение нормативных и законодательных требований к защите информации.[1] Именно благодаря грамотно построенным процессам аутентификации и управления доступом организации способны минимизировать риски несанкционированного доступа к чувствительным данным и поддерживать высокий уровень безопасности информационных систем.

Традиционно, аутентификация осуществляется с помощью чего-то, что пользователь знает (например, пароль), чего-то, что у пользователя есть (например, смарт-карта или токен), или чего-то, что является частью пользователя (биометрия, например отпечатки пальцев). Несмотря на широкое распространение, каждый из этих методов имеет свои недостатки. Пароли могут быть подобраны или украдены, токены потеряны, а биометрические данные скопированы или подделаны.

Традиционные методы аутентификации включают в себя использование паролей, физических устройств, таких как смарт-карты или токены, и биометрических данных, например отпечатков пальцев. Эти методы на протяжении многих лет служили основой для проверки подлинности пользователей, предоставляя различные уровни защиты и удобства. Пароли, вероятно, самый распространенный метод, основанный на знании пользователя уникальной комбинации символов, которую можно ввести для доступа к системе. Однако,

несмотря на их широкое распространение, пароли подвержены множеству угроз, таких как фишинг, подбор пароля и социальная инженерия.

Физические устройства, такие как смарт-карты или токены, представляют собой еще один слой защиты, поскольку требуют от пользователя нечто, что он имеет. Эти устройства могут генерировать одноразовые пароли или использоваться в сочетании с пин-кодом для доступа к ресурсам. Такой подход значительно повышает безопасность, но влечет за собой дополнительные затраты и неудобства, связанные с необходимостью постоянно носить с собой эти устройства.

Биометрическая аутентификация использует уникальные физиологические или поведенческие характеристики человека, такие как отпечатки пальцев, геометрия лица, голос или даже рисунок радужки глаза, как средство идентификации. Биометрия предлагает высокий уровень безопасности и удобства, поскольку пользователям не нужно запоминать сложные пароли или носить с собой дополнительные устройства. Однако этот метод также имеет свои недостатки, включая возможность ошибок при считывании, проблемы с приватностью и потенциальную уязвимость перед биометрическим спуфингом.

В целом, традиционные методы аутентификации предоставляют основу для защиты доступа к системам и данным, но каждый из них имеет свои ограничения и уязвимости. Это подчеркивает необходимость постоянного развития и адаптации методов аутентификации для обеспечения надежной защиты в меняющемся технологическом ландшафте.

В ответ на ограничения традиционных методов развивается многофакторная аутентификация (MFA), которая сочетает два или более метода из разных категорий, значительно увеличивая уровень безопасности. Например, использование пароля в сочетании с одноразовым кодом, отправленным на мобильный телефон пользователя, значительно затрудняет несанкционированный доступ.

Многофакторная аутентификация, или MFA, представляет собой процесс, в котором для подтверждения идентичности пользователя требуется несколько методов аутентификации из разных категорий, что значительно повышает безопасность по сравнению с использованием одного метода. Этот подход основан на предположении, что даже если один из факторов будет скомпрометирован, шансы на то, что злоумышленник сможет обойти все уровни защиты, существенно снижаются. MFA обычно включает комбинацию чего-то, что известно пользователю (например, пароль или пин-код), чего-то, что у пользователя есть (например, смартфон или специальный токен), и чего-то, что является частью пользователя (например, биометрические данные).

Применение MFA начинается с использования традиционного пароля, что уже является стандартной практикой. Однако, в отличие от простой аутентификации по паролю, в процесс добавляется еще один или несколько дополнительных шагов. Это может быть одноразовый код, отправленный на мобильное устройство пользователя посредством SMS или специализированного приложения, или же запрос на подтверждение входа через приложение управления учетными записями. Для еще большей защиты может быть использован биометрический сканер, который проверяет уникальные физиологические характеристики пользователя, такие как отпечаток пальца, геометрия лица или скан радужки глаза.

Таким образом, даже если злоумышленникам удастся узнать или угадать пароль пользователя, без доступа к физическому устройству или биометрическим данным они не смогут получить доступ к защищенной информации. Эта методика особенно ценна в условиях

постоянно растущего числа попыток фишинга и других видов кибератак, направленных на получение конфиденциальных данных пользователя. MFA эффективно укрепляет защиту, минимизируя риски, связанные с утечкой данных и несанкционированным доступом, и является критически важным элементом современной стратегии информационной безопасности.

С развитием технологий биометрическая аутентификация становится все более популярной благодаря своей удобству и высокому уровню безопасности. Современные биометрические системы используют не только отпечатки пальцев, но и распознавание лиц, голоса, радужки глаза и даже поведенческую биометрию, такую как динамика набора текста или образец движения мыши.

Биометрическая аутентификация представляет собой метод верификации идентичности пользователя на основе уникальных физиологических или поведенческих характеристик. В отличие от традиционных подходов, основанных на знании (например, пароли) или владении (например, ключи или карты), биометрическая аутентификация исключает необходимость помнить сложные пароли или носить с собой физические устройства. Этот метод использует уникальные признаки человека, такие как отпечатки пальцев, геометрия лица, сканирование радужки глаза, распознавание голоса или даже уникальные характеристики походки. Благодаря тому, что каждый человек обладает уникальными биометрическими данными, этот метод обеспечивает высокий уровень безопасности и удобства.

Применение биометрической аутентификации охватывает широкий спектр сценариев, от разблокировки смартфонов и ноутбуков до доступа в защищенные зоны и системы. Процесс аутентификации происходит путем сравнения представленных биометрических данных с предварительно сохраненными образцами в базе данных. Если система обнаруживает совпадение, доступ предоставляется.[2] Это не только ускоряет процесс аутентификации, но и значительно повышает его надежность, поскольку подделка биометрических данных значительно сложнее, чем кража пароля или физического токена.

Однако, несмотря на преимущества, биометрическая аутентификация имеет и свои недостатки. Ошибки при считывании данных, изменения биометрических характеристик со временем и потенциальные вопросы конфиденциальности и приватности данных требуют тщательного рассмотрения и адресации. Кроме того, существует риск централизованного хранения биометрических данных, что может стать мишенью для кибератак. Тем не менее, с постоянным развитием технологий и усилениями в области защиты данных, биометрическая аутентификация продолжает зарекомендовать себя как один из самых перспективных и надежных методов проверки подлинности пользователя.

В последнее время блокчейн технологии и децентрализованные идентификаторы начинают активно применяться в сфере аутентификации и управления доступом. Децентрализованные идентификаторы (DID) — это новый тип идентификатора, который позволяет пользователю полностью контролировать свою цифровую идентичность без необходимости полагаться на центральный авторитет. Это означает, что пользователи могут управлять своей идентичностью и данными лично, без посредников. Блокчейн обеспечивает безопасность и непрерывность этого процесса, записывая каждое изменение в распределенный реестр, который практически невозможно подделать или изменить.

В сфере аутентификации и управления доступом наблюдается стремительное развитие децентрализованных идентификаторов и применение блокчейн технологий. Эти инновации

представляют собой переломный момент, изменяя фундаментальные принципы управления цифровой идентичностью и предоставления доступа к ресурсам. Суть децентрализованных идентификаторов заключается в предоставлении пользователю полного контроля над его цифровой идентичностью, что радикально отличается от традиционных подходов, при которых управление идентификаторами осуществляется централизованными ауторитетами, такими как сервисы электронной почты, социальные сети или корпоративные системы.

Блокчейн технологии, служащие основой для децентрализованных идентификаторов, обеспечивают неизменяемость и прозрачность всей системы. Записи о цифровой идентичности пользователя размещаются в блокчейне, обеспечивая высокий уровень безопасности и защиты от подделок, поскольку изменение какой-либо информации в одном блоке потребует изменений во всех последующих блоках, что практически невозможно без обнаружения. Таким образом, блокчейн позволяет создать надежную и прозрачную систему управления идентификаторами, где пользователь может легко подтвердить свою идентичность, не беспокоясь о рисках утечки данных или несанкционированного доступа.

Децентрализованные идентификаторы и блокчейн технологии вносят значительный вклад в улучшение методов аутентификации и управления доступом, предлагая новые возможности для обеспечения приватности и безопасности в цифровом мире. Эти технологии дают пользователю возможность взять управление своей цифровой идентичностью в свои руки, что является значительным шагом вперед по сравнению с традиционными централизованными системами, часто подверженными риску централизованных атак и утечек данных. Применение децентрализованных подходов и блокчейн технологий в аутентификации и управлении доступом открывает новые горизонты для создания более безопасных, удобных и контролируемых пользователем систем идентификации.

Адаптивная аутентификация — это подход, который использует контекстную информацию (например, местоположение, время входа, используемое устройство) для оценки уровня риска каждой попытки доступа и адаптации требований к аутентификации соответственно. Это может включать требование дополнительных факторов аутентификации в ситуациях, когда уровень риска высок, или упрощение процесса аутентификации, когда риск низкий. Адаптивная аутентификация и управление доступом позволяют создать баланс между удобством для пользователя и необходимостью обеспечения безопасности. Адаптивная аутентификация и управление доступом представляют собой передовой подход к обеспечению безопасности, который учитывает динамичность современного цифрового мира. Эта методика отличается от традиционных статичных систем тем, что она анализирует ряд контекстных факторов во время попытки доступа пользователя к ресурсам или системам, позволяя таким образом динамически адаптировать требования к аутентификации. Эти факторы могут включать местоположение пользователя, используемое устройство, время доступа и даже тип запрашиваемых данных или услуг.

Основываясь на анализе этих данных, система может определить уровень риска каждой отдельной попытки доступа и, соответственно, адаптировать механизмы аутентификации. Например, если пользователь пытается получить доступ из известного местоположения в обычное рабочее время с помощью устройства, которое регулярно используется для этих целей, система может снизить требования к аутентификации, сделав процесс входа более удобным. В противоположность, попытка входа с неизвестного устройства или из аномального местоположения может вызвать запрос на дополнительные факторы

аутентификации, такие как код подтверждения, отправленный на доверенное устройство, или даже биометрическую проверку.[4]

Этот интеллектуальный подход позволяет создать баланс между безопасностью и удобством для пользователя, повышая защиту без создания ненужных препятствий для легитимного доступа.[7] Адаптивная аутентификация и управление доступом также способствуют повышению общей безопасности системы, так как они позволяют мгновенно реагировать на подозрительные действия, минимизируя риск несанкционированного доступа и потенциальных угроз.

В эпоху, когда кибератаки становятся все более изощренными, а методы взлома постоянно эволюционируют, адаптивная аутентификация и управление доступом представляют собой ключевые инструменты для защиты цифровых активов. Они обеспечивают организациям гибкость и мощные средства защиты, необходимые для эффективного реагирования на постоянно меняющуюся угрозу безопасности в цифровом пространстве.

Управление доступом играет ключевую роль в предотвращении утечек данных. Разграничение доступа к информационным ресурсам на основе ролей пользователей (RBAC), принцип наименьших привилегий и постоянный мониторинг и аудит действий пользователей — все это помогает минимизировать риск несанкционированного доступа и утечек данных. Эффективное управление доступом требует постоянного пересмотра и обновления политик доступа, чтобы они соответствовали меняющимся бизнес-процессам и угрозам безопасности.

Предотвращение утечки данных является одной из ключевых задач современной информационной безопасности, и управление доступом играет в этом процессе важнейшую роль. Эффективное управление доступом обеспечивает, чтобы каждый пользователь или система имели доступ только к тем данным и ресурсам, которые необходимы для выполнения их задач, тем самым снижая риск несанкционированного доступа к чувствительной информации.

В основе этого подхода лежит принцип наименьших привилегий, который предполагает предоставление пользователям минимально возможных прав и доступа, необходимых для их работы.[5] Это означает, что доступ к информации строго контролируется и ограничивается в соответствии с ролями и обязанностями пользователя в организации. Такой подход позволяет не только минимизировать возможности для утечки данных, но и упростить отслеживание и анализ действий пользователей в системе, что важно для выявления и предотвращения потенциальных угроз.

Кроме того, управление доступом включает в себя механизмы аутентификации и авторизации, которые гарантируют, что доступ к ресурсам получают только те пользователи, которые прошли надлежащую проверку и которым этот доступ явно разрешен. Эти механизмы могут включать в себя как традиционные методы, такие как пароли и PIN-коды, так и более современные, например многофакторную аутентификацию и биометрическую верификацию.

Для обеспечения долгосрочной защиты данных управление доступом должно быть динамичным и адаптироваться к изменениям в организационной структуре и технологическом ландшафте. Это включает в себя регулярный пересмотр и корректировку политик доступа, а также мониторинг и аудит системы на предмет аномальных действий, которые могут указывать на попытки несанкционированного доступа или внутренние угрозы.

Таким образом, управление доступом выступает в качестве многоуровневой защиты от утечки данных, сочетая в себе строгий контроль над правами доступа, продвинутые методы аутентификации и постоянный анализ действий пользователей. Эти меры, применяемые совместно, создают надежный барьер для защиты ценной информации организации от внешних и внутренних угроз.

В заключение, обеспечение безопасности в современном цифровом мире требует комплексного подхода к аутентификации и управлению доступом. Развитие технологий и появление новых угроз делают эти процессы не только актуальными, но и необходимыми для защиты цифровых активов и конфиденциальной информации. Мы рассмотрели различные аспекты аутентификации и управления доступом, начиная от традиционных методов, таких как использование паролей и биометрических данных, до современных подходов, включая многофакторную аутентификацию, адаптивную аутентификацию, а также применение децентрализованных идентификаторов и блокчейн технологий.

Важность адаптации к новым технологиям и методикам обеспечения безопасности не может быть переоценена. Управление доступом и аутентификация являются критически важными компонентами защиты информации, которые помогают предотвращать несанкционированный доступ и утечку данных. Эффективная реализация этих процессов требует постоянного пересмотра и обновления, чтобы соответствовать меняющимся условиям и угрозам безопасности.

Список литературы

1. Krasov A. et al. Using mathematical forecasting methods to estimate the load on the computing power of the IoT network //The 4th International Conference on Future Networks and Distributed Systems (ICFNDS). – 2020. – С. 1-6.
2. Гельфанд А. М. и др. Интернет вещей (IoT): Угрозы безопасности и конфиденциальности//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 215-220.
3. Гельфанд А. М. и др. Исследование распределенного механизма безопасности для устройств интернета вещей с ограниченными ресурсами//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 321-326.
4. Косов Н. А. и др. Анализ методов машинного обучения для детектирования аномалий в сетевом трафике//Цифровизация образования: теоретические и прикладные исследования современной науки. – 2021. – С. 33-37.
5. Косов Н. А., Тимофеев Р. С. Сравнение методов обучения свёрточных нейронных сетей//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 526-530.
6. Косов Н.А., Мазепин П.С., Гришин Н.А. Применение нейронных сетей для автоматизации тестирования программного обеспечения //Наукосфера. – 2020. – №. 6. – С. 152-156.
7. Штеренберг С.И. Методика построения защищенных систем искусственного интеллекта для проведения электроретинографии в офтальмологии //Офтальмохирургия. – 2022. – №. 4s. – С. 51-57.

References

1. Krasov A. et al. Using mathematical forecasting methods to estimate the load on the computing power of the IoT network //The 4th International Conference on Future Networks and Distributed Systems (ICFNDS). – 2020. – pp. 1-6.
2. Gelfand A.M. et al. Internet of things (IoT): security and privacy threats//Actual problems of infotelecommunications in science and education (APINO 2021). – 2021. – pp. 215-220.
3. Gelfand A.M. et al. Investigation of a distributed security mechanism for Internet of Things devices with limited resources //Actual problems of infotelecommunications in science and education (APINO 2020). – 2020. – pp. 321-326.
4. Kosov N. A. et al. Analysis of machine learning methods for detecting anomalies in network traffic //Digitalization of education: theoretical and applied research of modern science. – 2021. – pp. 33-37.
5. Kosov N.A., Timofeev R.S. Comparison of training methods for convolutional neural networks//Actual problems of infotelecommunications in science and education (APINO 2021). – 2021. – pp. 526-530.
6. KOSOV N.A., MAZEPIN P.S., GRISHIN N.A. Application of neural networks for software testing automation //The sciencosphere. - 2020. – No. 6. – pp. 152-156.
7. Shterenberg S. I. Methods of constructing protected artificial intelligence systems for conducting electroretinography in ophthalmology //OPHTHALMOSURGERY. – 2022. – No. 4s. – pp. 51-57.