УДК 004.001

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПРОЦЕССА АУТЕНТИФИКАЦИИ С ИСПОЛЬЗОВАНИЕМ ДОПОЛНИТЕЛЬНЫХ ФАКТОРОВ

С.А. Зайкова

Учреждение образования «Гродненский государственный университет имени Янки Купалы», Гродно, Беларусь

Аннотация. Разработана новая многофакторная система аутентификации, где метод с использованием аудиопотоков используется в качестве второго фактора. Исследована область возможного применения, определены необходимые для поддержки клиентского приложения браузеры. Предложен алгоритм аутентификации, алгоритм сравнения двух тоновых наборов оцифрованных аудиопотоков. Спроектированы и реализованы программные средства для реализации взаимодействия между внутренними компонентами новой корпоративной системы, рассмотрены улучшенные методы защиты передаваемых данных. Основные идеи метода включают в себя: гарантию присутствия пользователя в точке входа; возможность автоматизации процесса ввода одноразового пароля для сотрудников компании. Предусмотрена интеграция с коммуникационной платформой Twilio. Тестирование успешного применения предложенного решения показало успешность и эффективность применяемого метода, как дополнительного фактора во внутреннюю систему ИТ-компании.

Ключевые слова: многофакторная аутентификация; обеспечение безопасности; программные средства; аудиопотоки; корпоративная система, точка входа, программный интерфейс.

ENSURING THE SECURITY OF THE AUTHENTICATION PROCESS USING ADDITIONAL FACTORS

S.A. Zaikova

Yanka Kupala State University of Grodno, Belarus

Abstract. A new multi-factor authentication system has been developed, where the method using audio streams is used as the second factor. The area of possible application has been investigated, the browsers required to support the client application have been identified. An authentication algorithm and an algorithm for comparing two sets of tones from digitized audio streams are proposed. Software tools have been designed and implemented to facilitate interaction between the internal components of the new corporate system, and improved methods for protecting transmitted data have been considered. The main ideas of the method include: guaranteeing the user's presence at the entry point; the ability to automate the process of entering a one-time password for company employees. Integration with the Twilio communication platform is provided. Testing the successful application of the proposed solution demonstrated the success and effectiveness of the applied method as an additional factor in the internal system of an IT company.

Keywords: multi-factor authentication; security assurance; software tools; audio streams; corporate system; entry point; software interface

Введение

В настоящее время существует множество различных систем аутентификации, включая корпоративные системы, но не каждая из них гарантирует наличие сотрудника в точке входа. Как один из способов решения данной проблемы, можно считать применение специализированных программных средств для ограничения ввода одноразового пароля, в рамках ограниченного промежутка времени [1, 2]. Следует отметить, что такие меры могут стать причиной неудачных попыток аутентификации и ситуации, когда сотрудники компании начинают игнорировать проблемный фактор, предпочитают быстрый альтернативный вариант. Наиболее пренебрежительные пользователи выбирают вход с помощью кодов восстановления. При рассмотрении других вариантов, возможно использование переносных аппаратных средств, например, для сканирования одноразового пароля в формате QR-кода. Однако, следует признать, что этот метод также не всегда удобен по нескольким причинам, и зачастую не оправдывает себя, потому что пользователь, знакомый с технологией QR-кодов, может потребовать дополнительного обучения. Поэтому современные системы аутентификации вынуждены предлагать альтернативные варианты входа для компаний и организаций.

Основная часть

Аутентификация на основе аудиопотоков решает указанную выше проблему и является удобной альтернативой, которая исключает человеческий фактор из цепочки проверки подлинности. В этом случае сотрудник компании не производит ввод одноразового пароля вручную. Этот метод аутентификации происходит быстро, достаточно лишь поднести источник звука к микрофону. Таким образом, данный метод не только обеспечивает безопасность аутентификации, но также и гарантирует присутствие сотрудника компании в точке входа, так как вероятность передачи токена пользователем посторонним либо злоумышленникам практически исключена.

Аутентификация на основе аудиопотоков может быть произведена на большом количестве устройств. Данный метод актуален в том числе, для корпоративных веб-приложений, которые используют второй фактор для аутентификации. Если руководители компаний, организаций сталкиваются с такой проблемой, как «усталость от безопасности», аутентификация на основе аудиопотоков позволит сотрудникам проходить процесс авторизации быстрее и проще. Кроме того, если программному сервису необходимо защититься от умышленной передачи пользователем реквизитов для входа, такой способ аутентификации заставит сотрудника компании находиться физически рядом с точкой логина к ресурсу, требовательному к процессам информационной безопасности. Например, в ситуации передачи доступа к критически важным данным и ресурсам посторонним лицам, находящимся удаленно физически.

Поддерживая постоянный сеанс связи, можно производить аутентификацию данным методом длительно. Например, если системе требуется гарантировать присутствие пользователя в течении продолжительного периода времени, то, изменив конфигурацию метода, аудиопоток можно не прекращать и производить аутентификацию постоянно. Это позволит осуществлять доступ только во время проигрывания аудиопотока. Целевая аудитория такого приложения должна понимать, как совершить данную аутентификацию. Если бизнес-требования ориентированы на поддержку широкого круга пользователей, данный метод может быть проблематичным, так как требует несколько активных сессий.

Спроектированная система удовлетворяет следующим требованиям: предложенное решение поддерживаться популярными браузерами. Корректно обрабатывает все этапы аутентификации. Отображает актуальный интерфейс приложения. Интегрируется с другими приложениями и системой управления компанией, предприятием. Поддерживаются GSM и WebRTC методы связи. Используемые библиотеки имеют открытый исходный код.

В процессе разработки учтено обстоятельство о том, что запись и воспроизведение аудио поддерживается большинством персональных устройств, и, таким образом, аутентификация на основе аудиопотоков должна поддерживаться большим количеством пользователей, сотрудников компании. Для передачи аудио необходимо создать аудиопоток между клиентским приложением и серверным. Если клиентское приложение запущено в системе, не поддерживающей аутентификацию на основе аудиопотоков, приложение должно корректно обрабатывать исключительные ситуации и оповещать пользователя, что аутентификация невозможна.

Клиентское приложение в системе выполняет две функции: отображает пользователю интерфейс и взаимодействует с сервером; взаимодействует с коммуникационной платформой. Коммуникационная платформа, в свою очередь, устанавливает связь с устройством пользователя для проигрывания аудиоряда в зависимости от выбранных настроек. Поведение и способ связи определяется через API платформы. Серверное приложение в предложенной схеме управляет процессом аутентификации: генерирует аудиофайл и инициализирует вызов через платформу, после чего взаимодействует через события с клиентским приложением. Ссылка на аудиофайл и идентификатор устройства пользователя используются в объекте конфигурации, передаваемом коммуникационной платформе. Во время вызова сервер обрабатывает асинхронные запросы от платформы.

На первом этапе парольного фактора логин и пароль пользователя отправляются POST запросом. Далее, сервер запрашивает из базы данных информацию о пользователе и сохраняет ее в хэш-хранилище. Взаимодействие между базой и сервером защищено SSL-шифрованием, срок действия аутентификационного токена устанавливается в зависимости от требований конкретной системы. Для всего процесса аутентификации требуется логин, пароль (парольный хэш) пользователя и его идентификаторы ранее зарегистрированных устройств. После валидации полученных реквизитов пользователя сервер отправляет ответ со статусом и списком доступных методов.

После того, как метод выбран, сервер генерирует аудиоряд с помощью набора сэмплов разных частот и функции, объединяющей их в один файл. Далее, сервер создает конфигурацию, которая состоит из: одноразовой ссылки для выгрузки аудиофайла, идентификатора устройства, инструкций, описывающих поведение платформы во время коммуникации и ссылки для обратных вызовов.

Объект с инструкциями будет передаваться коммуникационной платформе посредством POST запроса. После выгрузки аудиофайла, платформа инициирует коммуникацию со вторым устройством пользователя. Максимальную задержку после начала проигрывания аудиоряда и принятия аудиопотока и количество повторений были установлены с ограничением в двойном повторении.

В качестве коммуникационной платформы в разработанной системе выступает API-сервис Twilio, предоставляющий управление большим выбором различных методов связи. Предоставляя управление своим API через язык разметки TwiML, сервис позволяет создавать программируемые вызовы, определенные в требованиях к разработанному решению.

Заключение

Результаты проведенного исследования несут в себе практическую значимость, как один из эффективных способов, гарантирующих присутствие сотрудника в точке входа, и решают одну из проблем безопасности современных методов аутентификации. Предложенное программное решение учитывает то обстоятельство, что необходимые для аутентификации воспроизводящие и записывающие звук компоненты есть в большом количестве устройств, имеющих выход в сеть интернет. На следующем этапе проектирования и разработки модулей системы возможно использовать дополнительные программные инструменты на основе нейронных сетей, в том числе для отсеивания постороннего шума, так как набор используемых частот известен заранее.

Список использованных источников

1. Шнайдер Б. (2023) Взломать все. Москва, Издательство «Альпина паблишер».
2. Афанасьев А. А. и др. (2012) Теория и практика обеспечения безопасного доступа. Москва. Издательство «Горячая линия–Телеком».

References

1. Shnaider B (2023) Hack everything. Moscow. Alpina Publishing House (in Russian).
2. Afanasiev A. A. and oth., (2012) Theory and practice of ensuring secure access. Moscow. Hotline - Telecom Publishing House (in Russian).

Сведения об авторе

Зайкова С.А., канд. физ.-мат. наук, доц., доцент каф., УО «Гродненский государственный университет имени Янки Купалы», sunny@mf.grsu.by.

Information about the author

Zaikova S., Cand. Sci. (Phys. and Math.), Associate Professor of the Department, Yanka Kupala State University of Grodno, Republic of Belarus, sunny@mf.grsu.by.