ПАРОЛЬНАЯ АУТЕНТИФИКАЦИЯ В ВИРТУАЛЬНОЙ РЕАЛЬНОСТИ

Студент кафедры интеллектуальных систем факультета радиофизики и компьютерных технологий Манцевича А.В.

Научный руководитель - кандидат ф-м. наук Головатый А.И.

Белорусский государственный университет

Минск, Беларусь

Виртуальная реальность – это одно из самых перспективных направлений развития современных технологий. С каждым годом VR-гарнитуры становятся все более доступными для широкой аудитории, что приводит к увеличению спроса на программные продукты, поддерживающие данную технологию.

В настоящее время в разработке находится много VR-проектов, в которых возникает необходимость разграничения доступа к функциональным возможностям. Такие приложения включают в себя конфиденциальные данные или функции, доступные ограниченному числу пользователей.

Аутентификация играет особую роль при управлении доступом к определенным функциям приложения, которыми может воспользоваться определённое число пользователей. Наиболее актуальна данная тема в многопользовательских играх и приложениях, где аутентификация необходима для обеспечения безопасности пользовательских данных и ограничения доступа к тем или иным виртуальным сценам.

Некоторые образовательные платформы и тренажеры, поддерживающие виртуальную реальность, должны включать в себя процесс аутентификации. Например, при обучении хирургов и военных данный процесс позволит обеспечить безопасный и конфиденциальный доступ к обучающим материалам и предотвратить утечку секретной информации.

Аутентификация в виртуальной реальности может быть использована как родительский контроль: для фильтрации контента в виртуальной реальности, чтобы предотвратить доступ к неуместному или нежелательному материалу.

В связи с этим возникает необходимость в разработке методов аутентификации, которые не только позволят обезопасить данные, но и обеспечат полное погружение в виртуальную реальность.

В ходе анализа существующих методологий аутентификации в виртуальной реальности было выделено три основных типа аутентификации: на факторе знаний, биометрическая и поведенческая. [2]

Поскольку методы аутентификации, основанные на факторе знаний, являются часто используемыми, рассмотрим их более подробно.

В подобного рода системах проверка осуществляется путем ввода PIN-кода или буквенно-цифрового пароля перед тем, как предоставить пользователю весь необходимый функционал. Как правило, создаются виртуальные клавиатуры или 3D модели, позволяющие ввести необходимую комбинацию символов. Данный тип аутентификации позволяет разработчикам использовать различного рода интерактивные системы, которые обеспечат эффект полного присутствия в виртуальном мире: кодовые замки, клавиатуры и др. (рисунок 1).

Рисунок 1. Примеры интерактивных систем аутентификации в виртуальной реальности.

Однако такие методы имеют и свои недостатки. Пароли могут быть подвержены утечкам и взлому, особенно если они представляют собой комбинации из небольшого количества символов. Кроме этого, некоторые методы могут быть непрактичны, так как пользователь вынужден затратить большое количество времени для ввода необходимой комбинации.

Ключевым аспектом защиты подобного рода систем является хранение паролей. Самый простой способ – это запись пароля в базу данных в незашифрованном виде. Таким образом, при попытке пользователя пройти аутентификацию будет сравниваться вводимая строка символов с той строкой, которая храниться в базе данных.

В этом случае есть большой риск того, что злоумышленники смогут получить информацию из базы данных. Например, недобросовестный пользователь системы с высоким уровнем доступа может скачать необходимую информацию и воспользоваться для корыстных целей. Кроме того, для кражи паролей могут быть использованы учетные данные этого пользователя. Другой вариант – злоумышленники воспользуются уязвимостями в используемом для хранения данных ПО. Таким образом, хранение паролей в открытом виде подвергает пользователя большому риску, связанному с утечкой аутентификационных данных.

В большинстве информационных систем подобного рода риски устраняются при помощи криптографической защиты.

Хэш (англ. hash – «превращать в фарш», «мешанина») или как его еще называют, хэш-функция - это специальные криптографические алгоритмы, превращающие любые данные в строку битов фиксированной длинны предсказуемым, но необратимым образом. То есть, одни и те же данные всегда будут преобразованы в один и тот же набор битов, который совершенно невозможно преобразовать в исходный набор данных. [3]

На первый взгляд может показаться, что если пропустить пароль через криптографическую хэш-функцию, то он будет в безопасности. Однако в

действительности это совершенно не так. Существует множество видов атак, которые позволяют восстановить пароли из простых хэш-кодов.

Если у нескольких пользователей один и тот же пароль, хэш-коды их функций будут идентичными. Такого рода атаки можно лишить эффективности, если внести в каждый хэш что-то уникальное. Это позволит исключить одинаковые хэш-коды. Даже в случае, если попадаются идентичные хэши, это совершенно не означает, что они соответствуют одному и тому же паролю.

Соль – это набор случайных символов, который каждый раз перед прохождением через хэш-функцию добавляется к паролю. [4]

Соль должна быть своя для каждого пользователя и пароля, поэтому набор символов должен быть достаточно длинным. Каждый раз, когда пользователь создает учетную запись или изменяет свой пароль, его нужно захэшировать с помощью новой случайной соли.

Алгоритм сохранения пароля представлен на рисунке 2.

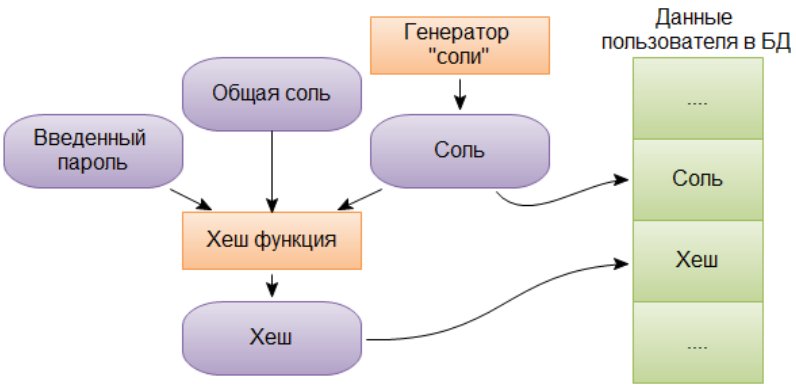

Рисунок 2. Сохранение пароля в базу данных.

Алгоритм проверки подлинности пароля представлен на рисунке 3.

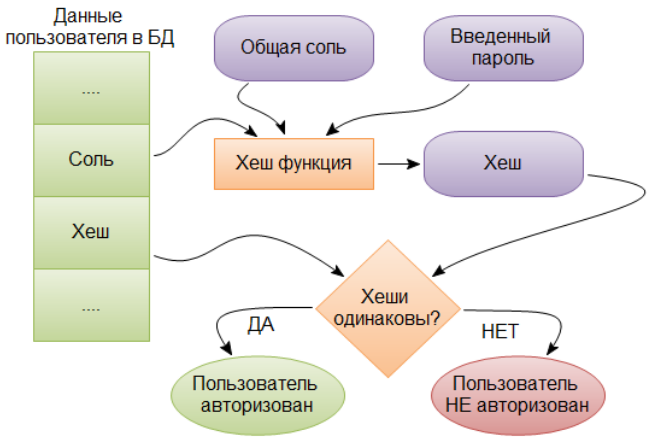

Рисунок 3. Проверка подлинности пароля.

Для реализации аутентификации в виртуальной реальности было принято решение создать кодовый замок, который работает по следующему принципу: пользователь, нажимая на кнопки контроллера движения рук, должен крутить каждый цифровой диск до тех пор, пока не будет установлена необходимая цифра. Каждый диск представляет из себя 10-угольную призму, на гранях которой расположены цифры от 0 до 9. Использовав несколько таких дисков, можно сформировать полноценный кодовый замок, регулируя тем самым длину необходимой комбинации.

Чтобы пользователь смог набрать необходимую комбинацию на кодовом замке, цифровые диски должны вращаться, поэтому возникает необходимость в использовании контроллеров движения рук. Стоит отметить, что гарнитуры, в комплектацию которых не входят подобного рода контроллеры, не будут поддерживать данную систему аутентификации.

Таким образом был сформирован шестизначный кодовый замок, представленный на рисунке 4.

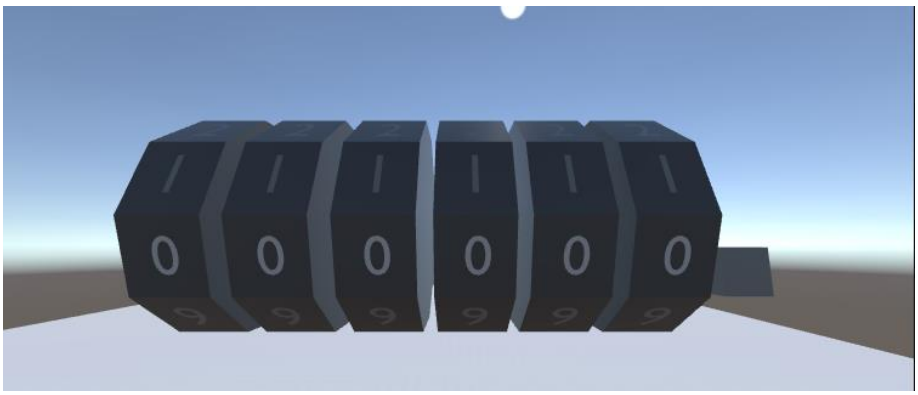

Рисунок 4. Кодовый замок.

Нажав на копку, пользователь запускает реализованный на практике алгоритм, который представлен на рисунке 5.

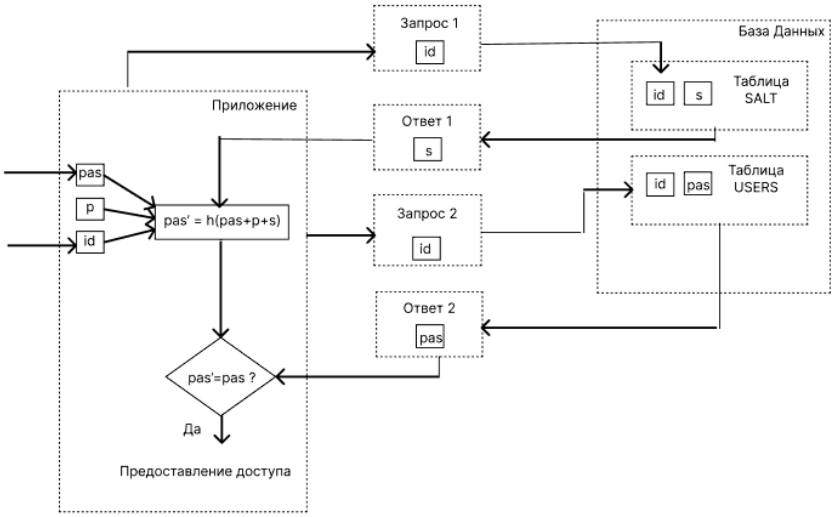

Рисунок 5. Схема работы алгоритма.

Аутентификация играет большую роль в обеспечении защиты и конфиденциальности данных, поэтому этой теме необходимо уделить особое внимание при разработке VR-приложений, которые подразумевают разграничение доступа пользователей.

Простота реализации и логическая ясность принципов работы алгоритмов, основанных на факторе знаний, делают системы парольной

аутентификации самыми популярными. Несмотря на большое количество уязвимостей, парольная аутентификация по-прежнему остается актуальной и используется в большинстве информационных систем.

Таким образом, была разработана система аутентификации, которая может быть интегрирована в виртуальную реальность. Данная система не лишена недостатков, однако благодаря ей разработчики приложений, поддерживающих данную технологию, смогут реализовать алгоритм авторизации, который позволит пользователям полностью окунуться в виртуальный мир.

Литература

1. Линовес Дж. Виртуальная реальность в Unity. Москва: ДМК, 2016.
2. Bertocci. V., Authenticating Users in Your VR Apps / Vittorio Bertocci // Official website of the company "Okta" [Electronic recource]. – 2022. – Mode of access: https://auth0.com/blog/authenticating-users-in-your-vr-apps/. -Date of acces: 14.12.2023
3. Donohue B. Чудеса хэширования / Brian Donohue. // Официальный сайт АО «Лаборатория Касперского» [Электронный ресурс]. – 2014. – Режим доступа: https://www.kaspersky.ru/blog/the-wonders-of-hashing/3633/. Дата доступа: 14.12.2023
4. «Интернет Технологии.ру» [Электронный ресурс]: «Соленое» хеширование паролей: делаем правильно. – 2020. – Режим доступа: https://www.internet-technologies.ru/articles/solenoe-heshirovanie-paroley-delaem-pravilno.html?ysclid=lq6gt95gr6814210196#header-9283-3. – Дата доступа: 14.12.2023