ИНТЕГРАЦИЯ В ВЕБ-ПРИЛОЖЕНИЯ АВТОРИЗАЦИИ ЛИЧНОСТИ ПО БИОМЕТРИЧЕСКИМ ПРИЗНАКАМ

И.Е. Бросалин, Н.Н. Минакова
Алтайский государственный университет, г. Барнаул

В информационной безопасности ограничение доступа является одним из главных инструментов обеспечением конфиденциальности, так злоумышленник, не знающий логин и пароль от аккаунта электронной почты, не сможет получить доступ к ней. Тем не менее есть ситуации, когда необходимо и ограничить доступ, и подтвердить личность человека для этого используются специальные пропуски, показываемые охраннику на контрольно-пропускном пункте, что актуально для режимных предприятий.

Актуальность проблемы идентификации личности подтверждается развитием технологий позволяющие это сделать, в качестве примера можно привести сканеры РОГ (радужная оболочка глаза) Условно признаки по которым происходит идентификация можно разделить на биометрические и не биометрические. Первые используют уникальные характеристики человека такие как: РОГ, папиллярный узор, сетчатка глаза, а вторые искусственные признаки такие как: пароль, одноразовые коды.

Так сегодня на просторах интернета можно пройти авторизацию, используя пару логин и пароль, сотовый телефон, электронную почту, социальные сети, однако перечисленные средства авторизации не идеальны. Если злоумышленник получит доступ к электронной почте, сотовому телефону, то он сможет восстановить пароль или просто пройти без парольную авторизацию и получит доступ к аккаунту. Почему это так? Дело в том, что отправляется одноразовый код, который потом вводится в форму на сайте для восстановления пароля, который подтверждает только доступ к другому довольно надёжному источнику информации. К сожалению, доступ к надёжному источнику никак не подтверждает личность никоим образом, хотя часто бывает так, что не обязательно привязываться к личности. Другой плюс биометрии заключается в том, что можно подтвердить человечность пользователя, так как бот может отправить через форму одноразовый пароль, используя стандартные библиотеки для обмена HTTP заголовками.

Поэтому встаёт вопрос как заменить одноразовые коды, на что-то более надёжное. Заменить одно разовые коды это не такая большая проблема, так как меняется только код для функционала «восстановление пароля» и не больше, что является сравнительно

небольшой модификацией. Однако такой вопрос как интеграция является более комплексным и подразумевает использование биометрии не только для восстановления пароля, но и для других операций, что позволяет усилить контроль за действиями пользователями. Так следующим этапом внедрения может стать подтверждение человечности перед

Основной целью является анализ возможности интеграции идентификации личности по биометрическим признакам в веб-приложение, а также реализация возможных вариантов.

Были выделены следующие задачи:

1. Разработка альтернативы одноразовым кодам;
2. Анализ инструментов для сбора данных;
3. Рассмотрение вопросов применимости и интеграции с существующими решениями;
4. Написание веб-приложения для демонстрации основных возможностей предлагаемого решения.

Для того чтобы разработать альтернативу одноразовым кодам, необходимо понять, как пользователь будет пользоваться привычным сайтом (веб-приложением) со встроенной биометрии. Так рисунок 1 показывает ситуацию восстановления пароля с использованием биометрии. На нём можно увидеть действия пользователя, сервера, на котором происходит авторизация, а также действия, выполняемые js-кодом на стороне клиента для получения биометрических данных.

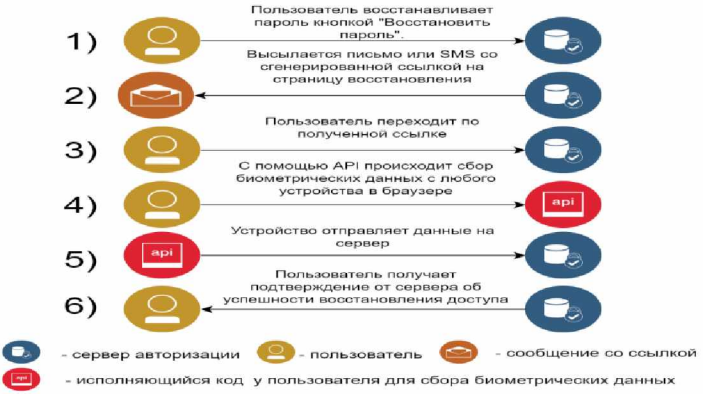

Рис. 1. Этапы восстановления пароля с использованием биометрии

Внедрение идентификации по биометрии не сильно увеличило количество этапов в рассматриваемой процедуре. Если убрать 4-ый пункт из рисунка 1, то можно получить этапы для восстановления пароля с помощью одноразовых паролей, однако в таком случае одноразовым паролем можно подтвердить только наличие доступа к почте или телефону, что никак не характеризует личность и не подтверждает, что именно человек выполняет действия для восстановления пароля.

В силу того, что разрабатываемое решение должно работать на всех устройствах был сделан выбор в пользу разработки решения, работающего в браузере которое впоследствии может быть встроено в другие веб-приложения. Для того чтобы получить биометрический признак с любого устройства нужно средствами браузера начать запись с микрофона голоса, сфотографировать пользователя, а ещё лучше записать видео со звуком для идентификации по нескольким биометрическим признакам. Относительно недавно появились решения, позволяющие выполнить описанные действия из браузера с любого устройства должного качества: Java Applet, Flash player, HTML5, WebRTC [1]. Два первых перечисленных не смогли выдержать конкуренции и не смогли устранить свои недостатки из-за чего рынок перестал массово их использовать. Введение в эксплуатацию HTML5 серьёзно расширило возможности браузера по взаимодействию с пользователями особенно в мультимедиен, так появился встроенный плеер, что позволило внедрить запись звука, фотографирование, съёмку видео и отдавать данные браузеру для дальнейшей работы.

WebRTC – протокол седьмого уровня для организации конференций из браузера появился почти одновременно с HTML5, так как на основе новых возможностей базировалась его работа. Из этого протокола можно взять функционал для сбора биометрии. На основе чего была разработана программа, рисунок 2. Так с помощью неё можно снять биометрические данные и отправить на сервер с помощью обычного POST запроса, однако локально продемонстрировать снятую информацию можно реализовав скачивание временно сохранённого файла с биометрией.

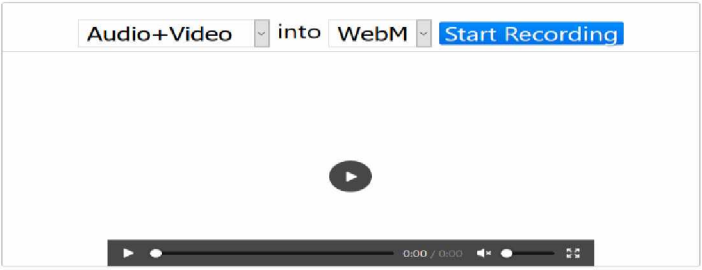

Рис. 2. Скриншот программы.

Интеграцию подобного решения можно провести путём подключения отдельного js-файла с кодом, для получения биометрических данных (применимо как замена одноразовых паролей и не более в силу неудобной поддержки кода) или вынести в отдельный web-сервис, что позволит наращивать функционал веб-приложения без смешивания кода и изолировать его от всего того, что не касается безопасности. Также этот способ удобен тем что можно развернуть отдельный сервер и обслуживать не одно веб-приложение, а несколько.

Была разработана альтернатива одноразовым кодам. Проведён анализ инструментов для сбора данных, а также рассмотрены вопросы применимости и интеграции с существующими решениями; Разработано веб-приложения для демонстрации основных возможностей предлагаемого решения.

Библиографический список

1. WebRTC, Flash RTMFP, Java Applet – три ведущих технологии для браузерных VoIP звонков [Электронный ресурс]. URL: http://club.cnews.ru/blogs/entry/webrtc_flash_java_ (дата обращения: 07.06.2018).
2. Минакова Н.Н. Методы технической и правовой защиты информации в сети Интернет // Н.Н. Минакова, В.В. Поляков, С.Н. Толстошеев – Барнаул, 2015.
3. Поляков В.В. Региональные аспекты технической и правовой защиты информации // В.В.Поляков, В.А. Трушин, В.В. Поляков и др. – Изд-во АлтГу, Барнаул, 2013.