УДК [004.93'1](http://teacode.com/online/udc/00/004.93'1.html)

**Использование облачной платформы аутентификации по подписи при создании защищённого мобильного приложения**

В.А. Пасенчук, СибАДИ, ФГБОУ ВПО «СибАДИ», г. Омск, Россия

***Аннотация.*** *Статья посвящена разработке инновационного метода аутентификации в мобильных приложениях, который заключается в анализе рукописного пароля. В статье приводится поэтапная разработка архитектуры сервиса, библиотеки, позволяющей внедрять аутентификацию по подписи в мобильные приложения, а также приложения, являющегося реализацией данной архитектуры. Архитектура сервиса включает ряд мер защиты информации, которые позволяют достичь высокой степени защищённости информации пользователей. Библиотека может быть использована при создании любых мобильных приложений для Android OS. Мобильное приложение SignPass является реализацией данной архитектуры.*

***Ключевые слова:*** *аутентификация по подписи, динамические характеристики подписи, защита от несанкционированного доступа, безопасность мобильных приложений, шифрование данных.*

Современные мобильные устройства представляют собой потенциальную цель для атак злоумышленников. Было установлено, что пользователи смартфонов и коммуникаторов как правило недооценивают риски попадания своих персональных данных в руки преступников с последующей продажей или использованием этой информации [1].

Как известно, хранение конфиденциальной информации на ненадёжных носителях может привести к краже данной информации.

Если для доступа к конфиденциальной информации требуется пароль или токен, а также при хранении носителя информации в сейф, то аутентификатор доступа к хранилищу информации отделим от владельца. Для повышения надёжности существует возможность использовать неотделимые от хозяина признаки, то есть его биометрические данные.

Одной из технологий, которая использует биометрическую идентификацию, является процедура установления личности с помощью методики идентификации по динамике написания слов (паролей).

Для того, чтобы определить, является ли субъект аутентифицированным пользователем, требуется сравнить его автограф с эталонным набором. Для получения эталонного набора требуется ввод не менее 10 образов подписи. В случае, если некоторые образцы имеют существенные отличия от прочих, требуется повторный ввод спорных образцов.

Сравнение осуществляется облачной платформой SignToLogin [2, 3]. Сопоставление введённой подписи с созданным образцом проводится системой SignToLogin по методике, разработанной в НТЦ «КАСИБ» на основе исследований Ложникова П.С и Сулавко А.Е. [2, 3, 4, 5, 7]. Согласно данной методике, сопоставление автографов осуществляется не по соответствию графического изображения, а по динамике написания подписи, которая в свою очередь напрямую связана с индивидуальными когнитивными процессами каждого человека [4]. Уровень ошибок первого и второго рода составляет 2% при ограничении общего числа зарегистрированных пользователей до 200 [3].

Под динамикой понимается совокупность вида подписи, скорости написания и давления пера (последний признак считывается с устройств, имеющих индуктивный экран и стилус).

Динамика написания подписи у каждого человека уникальна и её можно сравнить с отпечатками пальцев. Если графическое изображение будет достаточно схожим, но его введёт другой человек, система не аутентифицирует данного субъекта по причине различия динамических характеристик автографа.

Сущность сравнения подписи с эталонными значениями заключается в построении гипотез о степени схожести исследуемого образца с эталонными. Для сравнения предъявляемых биометрических образов с эталонными используется аппарат Байесовских сетей, в частности алгоритм последовательного применения модифицированной формулы гипотез Байеса, которая дает достаточно высокие результаты при идентификации образов в пространстве малоинформативных признаков [4, 5, 7, 8].

Концептуальная схема сервиса включает в себя взаимодействие мобильного устройства с сервером распознавания подписей SignToLogin с использованием сети Интернет (см. Рисунок 1).

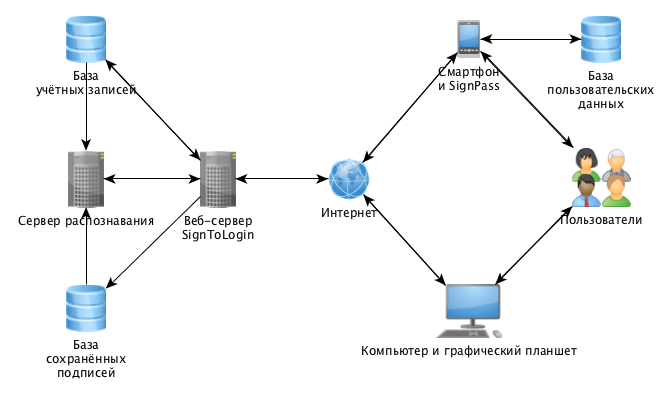


Рисунок 1. Схема архитектуры сервиса

Протокол регистрации включает в себя комплекс действий, обеспечивающих безопасность и удобство данного процесса (см. Рисунок 2). Данный процесс можно разделить на следующие этапы:

1. Проверка корректности ввода адреса.
2. Проверка наличия пользователя в системе.
3. Ввод эталонных образцов подписи.
4. Создание учётной записи на сервере.
5. Создание учётной записи на клиенте.

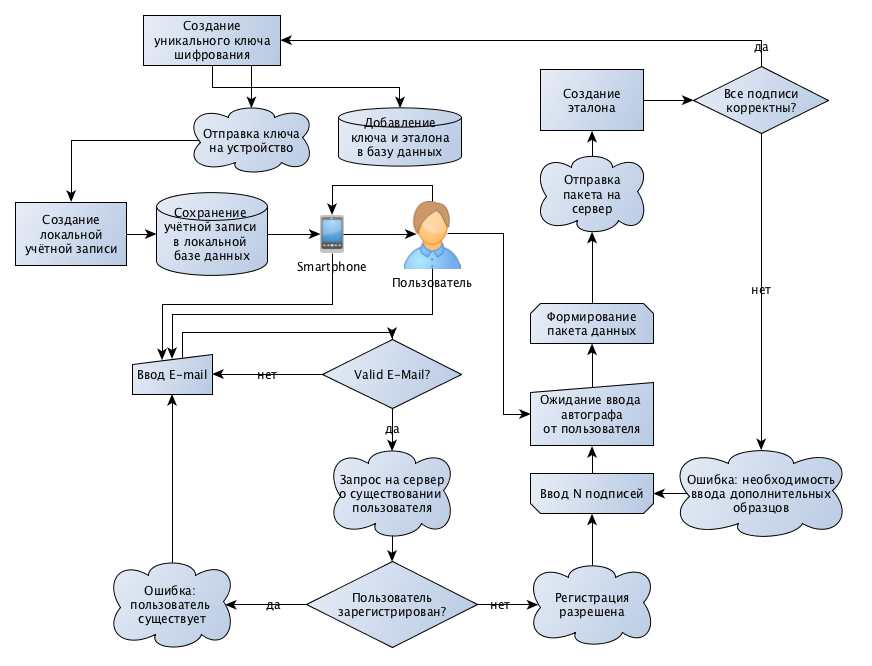


Рисунок 2. Протокол регистрации

Протокол авторизации имеет схожую структуру с протоколом регистрации (см. Рисунок 3). Данный процесс можно разделить на следующие этапы:

1. Проверка корректности ввода адреса.
2. Проверка наличия пользователя в системе.
3. Ввод подписи.
4. Отправка клиенту ключа шифрования.
5. Получение данных учётной записи на клиенте.

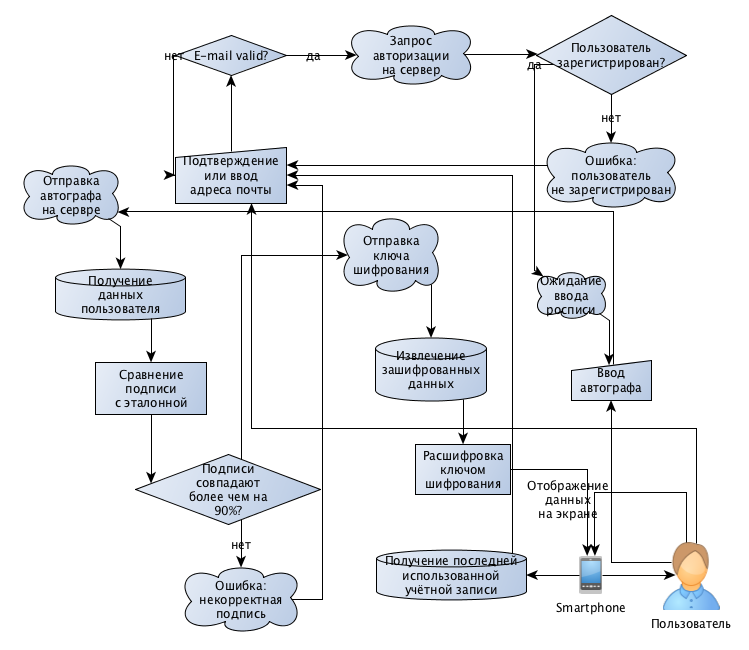


Рисунок 3. Протокол аутентификации

Для того, чтобы начать использование системы, требуется проделать следующие действия:

Пользователь регистрируется с помощью e-mail адреса и вводит не менее 10 образцов подписи.

Для обмена данных между облачным сервисом SignToLogin и мобильным приложением SignPass используется защищённый канал связи и REST API.

Облачная платформа верификации подписи SignToLogin анализирует образцы и создаёт эталон. Также, с помощью secure random, генерируется массив из 256 бит, предназначение которого – являться ключом шифрования для пользовательских данных.

Далее в базе данных сервиса создаётся запись, которая сопоставляет адрес электронной почты пользователя с эталоном его автографа и личным ключом шифрования (который был сгенерирован на предыдущем этапе).

Пользователю отправляется ключ шифрования, который используется для шифрования конфиденциальной информации (алгоритм AES 256/CBC/PKCS5Padding).

Создаётся локальная учётная запись в базе данных устройства. Введённая в приложения конфиденциальная информация (учётные данные для сторонних ресурсов) не отсылается на сервер, ключ шифрования не сохраняется в постоянной памяти устройства.

При входе в свою локальную учётную запись пользователь должен расписаться. Если SignToLogin подтверждает корректность подписи, то пользователю высылается ключ шифрования, с помощью которого можно получить доступ к своей конфиденциальной информации, сохранённой в приложении.

Безопасность сервиса обеспечивается следующими факторами:

Используемая размерность ключа шифрования (256 бит) является достаточной для защиты от полного перебора в абсолютном большинстве случаев.

Используемый алгоритм шифрования AES не имеет уязвимостей для всех основных видов криптоатак [9].

Использование режима шифрования CBC/PKCS5Padding гарантирует, что одинаковые блоки данных отобразятся в разные блоки шифртекста [10].

Конфиденциальные данные хранятся только на устройстве в зашифрованном виде.

Ни сервер SignToLogin, ни устройство (в момент, когда приложение не активно) не обладают достаточным набором информации для расшифровки данных. Таким образом, в случае кражи или утери устройства, злоумышленник не сможет получить доступ к конфиденциальной информации.

Алгоритм проверки подписи учитывает динамику ввода как по координатам, так и по давлению. Таким образом, злоумышленнику недостаточно знать, как выглядит подпись, требуется также соблюдать скорость ввода и давление, что существенно сокращает вероятность несанкционированного доступа.

Вся коммуникация с SignToLogin осуществляется через зашифрованный канал по протоколу HTTPS. Подлинность сертификатов SSL [11] может быть подтверждена соответствующими ресурсами.

Платформа SignToLogin была специально доработана для оптимальной и безопасной работы SignPass:

SSL-сертификаты были заменены на более известные, таким образом любое мобильное устройство на базе Android OS может проверить их подлинность.

Разработан алгоритм генерации, хранения и отправки на устройства ключа шифрования.

Порог совпадения подписи с эталоном был снижен с 95% до 90%, так как при вводе подписи с сенсорного экрана тяжело достичь настолько высокой стабильности ввода.

Существует отключаемый строгий режим повышенной безопасности, при котором переход приложения в неактивное состояние (сворачивание, полное перекрытие другим приложением, отключение экрана устройства) ведёт к автоматическому выходу из текущей учётной записи.

Приложение SignPass предназначено для хранения аутентификационных данных пользователей. Предполагается, что утеря подобной информации в большинстве случаев не может привести к большим убыткам, так как существует возможность восстановления этих данных с помощью мобильного телефона или электронной почты. Но попадание аутентифицирующей информации к третьим лицам может повлечь существенный вред владельцу этих данных.

Таким образом, приложение ориентировано на минимизацию вероятности ошибок второго рода, то есть классификации нарушителя как авторизованного пользователя. Ошибки первого рода (классификация авторизованного пользователя как нарушителя) не являются исключительной ситуацией и возникают в случае неаккуратного ввода подписи.

Также был проведён анализ решений конкурентов. Все предлагаемые решения используют анализ только динамических характеристик подписи. Из этого следует, что на текущий момент нет возможности выбрать продукт, способный осуществлять статический анализ документов (см. Таблица 1).

Таблица 1. Сравнение с продуктами конкурентов

|  |  |  |  |
| --- | --- | --- | --- |
| Характеристики | SignToLogin | CIC | SignDocDesktop |
| Не обязательное использование графического планшета | + | - | + |
| Анализ статического изображения подписи | - | - | - |
| Поддержка мобильных устройств | + | - | + |
| Анализ документов | - | - | - |
| Использование формы | + | + | + |
| Использование размера | + | + | + |
| Использование наклона | + | + | + |

У данной архитектуры также существуют следующие недостатки:

1. Стремление минимизировать угрозу попадания конфиденциальных данных третьим лицам привело к возникновению ряда недостатков:
2. Отсутствует возможность синхронизации данных с помощью облачных сервисов.
3. При утере или повреждении устройства данные также будут потеряны.
4. В случае травмы руки, которой осуществляется роспись, будет утеряна способность корректно ввести подпись. Таким образом, пользователь может потерять возможность доступа к своим данным.
5. Приложение требует доступа к Интернет для проверки подписи. Без доступа к Интернет пользователь не сможет получить ключ шифрования и просмотреть свои данные.
6. Невозможность осуществления статического анализа документов.

С точки зрения пользователя SignPass обладает следующими особенностями:

1. Личная надёжная записная книжка паролей SignPass, которая всегда под рукой и никто другой не сможет получить к ней доступ.
2. Аутентификация с использованием автографа.
3. Возможность иметь несколько учётных записей на одном устройстве.
4. Широкий перечень сервисов, для которых можно сохранить учётные данные. Для обеспечения удобства пользователя в приложении содержится большое количество пиктограмм для различных сервисов.
5. Создание, просмотр, редактирование, удаление записей.
6. Копирование аутентифицирующей информации в буфер обмена. Возможность отображения паролей на экране (из соображений безопасности данное действие требует подтверждение пользователя).
7. Отключаемый режим повышенной безопасности.
8. Поддержка различных конфигураций и размеров экрана
9. Наличие русской и английской локализации.
10. Возможности настройки отображения подписи.

***Заключение.*** В ходе выполнения данной работы была достигнута основная цель – создание альтернативного метода аутентификации для мобильных устройств. Предлагаемый метод использует в качестве аутентификатора рукописный пароль.

Результат работы – разработка и реализация архитектуры сервиса. Данная архитектура предлагает инновационный метод аутентификации, а также ряд мер, обеспечивающих высокую надёжность обработки и хранения данных.

SignPass является примером реализации архитектуры защищённого мобильного приложения. Отличием от других подобных приложений является способ аутентификации пользователя, так как SignPass – единственное приложение в Google Play, которое использует в качестве аутентификатора рукописный автограф.

Используемые технологии обработки и передачи информации, а также криптографические методы защиты информации позволяют обеспечить высокую степень сохранности данных пользователей.

***Библиографический список***

1. Quick, D. Digital Droplets: Microsoft SkyDrive Forensic Data Remnants // Future Generation Computer Systems / Quick, D., K.-K. R. Choo. – 2013. 29 (6). – P. 1378–1394.
2. Ложников П.С. Аналитическое исследование проблемы распознавания образов в пространстве малоинформативных признаков // Межотраслевая информационная служба / Ложников П.С., Сулавко А.Е. – 2014. №2 (167). – С.11-18.
3. Ложников П.С. Реализация метода верификации пользователей по динамике написания автографа на облачной платформе // Тезисы докладов и лекций международной школы-конференции «Математические проблемы информатики» 20-27 сентября 2013 г. – Омск: Изд-во ОмГТУ, 2013. – С. 29-31.
4. Ложников П.С. Облачная система идентификации пользователей по рукописным паролям «SIGNTOLOGIN» // Электроника инфо. – 2013. №6 (96). – С. 74-76.
5. Pavel Lozhnikov, Oksana Chernikova. Handwriting dynamics as a means of authentication / ICITST 2011: 6th International Conference on Internet Technology and Secured Transactions, 11-14 December 2011, Abu Dhabi, United Arab Emirates. – p. 176-179.
6. Епифанцев Б.Н. Алгоритм идентификации гипотез в пространстве малоинформативных признаков на основе последовательного применения формулы Байеса // Межотраслевая информационная служба / Епифанцев Б.Н., Ложников П.С., Сулавко А.Е. ФГУП «ВИМИ» - Москва : 2013, № 2. С. 57-62.
7. Сулавко А.Е. Метод сжатия собственных областей классов образов в пространстве малоинформативных признаков // Искусственный интеллект и принятие решений / Сулавко А.Е., Еременко А.В. - Москва: 2014, № 2. С. 95-102.
8. Daniel Kahneman Judgment under Uncertainty: Heuristics and Biases / Daniel Kahneman, et al. — 21st. — Cambridge University Press, 2005. — 555 p.
9. Баричев С.Г. 2.4.2. Стандарт AES. Алгоритм Rijdael // Основы современной криптографии. / Баричев С.Г., Гончаров В.В., Серов Р.Е. — М.: Горячая линия — Телеком, 2002. — С. 30—35.
10. Шнайер Б. 9.3. Режим сцепления блоков шифротекста // Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си = Applied Cryptography. Protocols, Algorithms and Source Code in C. — М.: Триумф, 2002. — С. 225—229. — 816 с.
11. T. Dierks The Secure Sockets Layer (SSL) // 1-st. — RTFM, Inc., August 2008. — № 1. — P. 207.
12. Иванов Ю.С. Обзор методов верификации личности по подписи и разработка программного обеспечения // Вестник научного общества студентов, аспирантов и молодых ученых / Иванов Ю.С., Авдеенко А.А.: Электронный выпуск. – 2014. – № 1. – 5 с.

Пасенчук Виктор Андреевич (Омск, Россия) – Сибирская государственная автомобильно-дорожная академия (СибАДИ). (644080 г. Омск, проспект Мира, 5).