DOI 10.37882/2223-2966.2023.09.39

АНАЛИЗ ПОДХОДОВ К РЕАЛИЗАЦИИ НЕПРЕРЫВНОЙ МНОГОФАКТОРНОЙ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ СМАРТФОНОВ

ANALYSIS OF APPROACHES TO THE IMPLEMENTATION OF CONTINUOUS MULTI-FACTOR AUTHENTICATION OF SMARTPHONE USERS

M. Shulga

Summary. Mobile devices and technologies become more popular and provide possibilities of persistence and calculation of comparable degree to personal desktop computers which allows users to save confidential personal info and interact with it on their devices. Security and protection of this type of information become more and more important because mobile devices are vulnerable for unauthorized access and theft. User's authentication provides access to legitimate users both at the entry point and continuously during the usage session and this authentication is a task of paramount importance. Implementation of this task became possible thanks to built-in sensors which ensure continuous implicit authentication while collecting behavioral biometric data and patterns. This article presents research on modern approaches for continuous authentication of users that uses behavioral biometric characteristics collected by phone's built-in sensors, considers open questions of implementing this authentication, ease of use and performance issues.

Keywords: sensor-based authentication, continuous authentication, mobile sensing, smartphone-based authentication.

Шульга Михаил Михайлович
Аспирант, Институт инженерной физики
mmshulga@yandex.ru

Аннотация. Мобильные устройства и технологии становятся все более популярными, предлагая возможности хранения и вычисления, сравнимые с настольными компьютерами, что позволяет пользователям хранить конфиденциальную и личную информацию и взаимодействовать с ней. Безопасность и защита такой личной информации становятся все более и более важными, поскольку мобильные устройства уязвимы для несанкционированного доступа или кражи. Аутентификация пользователя предоставляет доступ законным пользователям в точке входа и непрерывно в течение сеанса использования и является задачей первостепенной важности. Выполнение этой задачи стало возможным благодаря встроенным датчикам современных смартфонов, которые обеспечивают непрерывную и неявную аутентификацию пользователя, собирая поведенческие биометрические данные и характеристики. В статье представлено исследование современных подходов к непрерывной аутентификации пользователей с использованием поведенческих биометрических данных, фиксируемых встроенными датчиками смартфонов, рассмотрены открытые проблемы внедрения, удобства использования и производительности.

Ключевые слова: аутентификация на основе датчиков, непрерывная аутентификация, мобильное зондирование, аутентификация с помощью смартфона.

Современные технологии позволяют быстро улучшать такие характеристики смартфонов, как объем памяти и вычислительных ресурсов, что делает их бесценным инструментом для работы в Интернете и ведущей платформой для общения пользователей и взаимодействия с данными и мультимедиа различных форматов. Более того, современные услуги периферийных и облачных вычислений, доступные пользователям, увеличили зависимость от мобильных устройств в плане мобильности и удобства и произвели революцию в технологиях и методах проведения транзакций [1]. Непрерывная аутентификация пользователя — это неявный процесс проверки подлинности пользователя, основанный на регистрации поведенческих атрибутов с использованием ресурсов и встроенных датчиков мобильного устройства. Пользователи, как правило, вырабатывают отличительные модели поведения при использовании мобильных устройств, которые можно использовать для задачи аутентификации. Эти шаблоны неявно фиксируются в процессе взаимодействия пользователей со своими устройствами, и представляют собой поведенческие характеристики, вычисляемые на основе потока данных: действия пользователей, информация об окружающей среде и сенсорные данные. Методы непрерывной аутентификации работают в качестве поддержки традиционных способов аутентификации, таких как аутентификация по паролю или биометрическим данным, и могут инициировать процесс повторной аутентификации при обнаружении несанкционированного поведения.

Непрерывная аутентификация давно является областью повышенного интереса, и стала возможной благодаря развитию современных технологий и появлению возможностей создания более точных и специализированных датчиков. Использование методов аутентификации на основе датчиков обеспечивает удобный и эффективный контроль доступа для пользователей. В этой статье рассматриваются последние и современные ме-

тоды непрерывной аутентификации с использованием поведенческой биометрии, состояние и проблемы внедрения этих методов в современных смартфонах.

Традиционные и биометрические подходы. На сегодняшний день поставщики мобильных устройств используют схемы, основанные на знаниях и физиологических биометрических данных, в качестве основных методов доступа к устройству. Подходы, основанные на знаниях, полагаются на знания пользователя; т.е. пользователь должен предоставить определенную информацию, такую как числовой пароль, PIN-код, графическую последовательность или жест изображения [4], чтобы получить доступ к устройству [5]. Несмотря на свою простоту, легкость реализации и приемлемость для пользователей, такие подходы страдают рядом недостатков, таких как неудобство частого повторного входа (особенно когда используемые знания достаточно длинные, чтобы обеспечить надежную защиту) и уязвимость к таким атакам как серфинг через плечо [9]. Другой проблемой аутентификации на основе знаний является исходное предположение о наличии одинаковых требований безопасности для всех приложений (например, доступ к финансовым записям и отправка текстовых сообщений) имеют одинаковый уровень безопасности. Использование аутентификации, основанной на знаниях, на смартфонах не обеспечивает гарантии безопасности для конкретных приложений, особенно учитывая недавнее появление адаптируемой биометрической аутентификации, которая учитывает факторы окружающей среды для адаптации и выбора подходящих датчиков для аутентификации (например, с помощью датчика отпечатков пальцев, когда условия освещения не позволяют распознать лицо) [3]). Даже при использовании более сложных реализаций подходов, основанных на знаниях, например, реализации трехмерных графических паролей [5], которые легче запомнить и, возможно, обеспечивают большее пространство для пароля, они по-прежнему наследуют те же недостатки. В исследовании [9] показано, что графические последовательности (двумерные шаблоны) так же легче предсказать, как и текстовые пароли, поскольку 40% шаблонов начинаются с верхнего левого узла, а большинство пользователей используют пять узлов из девяти. Другой пример сложных схем, основанных на знаниях, представлен в работе [5], который включает в себя изменение цвета шести кругов путем неоднократного прикосновения к ним до семи раз. Как только все цвета кругов соответствуют правильной комбинации, авторизация пользователя подтверждается. Несмотря на то, что это обеспечивает более высокую безопасность (особенно при включении большего количества кругов и цветов), все же требуется запоминание таких сложных комбинаций, что является основным недостатком подходов, основанных на знаниях. Чтобы преодолеть потребность в запоминании сложных комбинаций, в [6] предложены жесты свободной формы (рисование) в качестве схемы проверки пользователя (пользователи должны вводить любой рисунок любым количеством пальцев). Авторами показано, что использование жестов свободной формы позволило сократить время входа в систему на 22 % по сравнению с текстовыми паролями, сохранив при этом более высокое удобство использования и пространство для поиска. Однако в авторы не рассматривали другие проблемы безопасности, такие как серфинг через плечо и smudge-атаки.

Многие исследователи пытались преодолеть основные проблемы аутентификации на основе знаний, сочетая эти методы с методами, основанными на биометрии. Использование биометрической информации повышает как точность, так и удобство использования процесса аутентификации. Такую интеграцию можно осуществить путем измерения динамики нажатия клавиш или жестов при подключении, изменении порядка или выборе изображений [7]. Недостатки подходов к аутентификации на основе знаний побуждают к использованию более надежных и простых схем аутентификации, таких как биометрия. Физиологическая биометрия обеспечивает бесспорную точность аутентификации пользователя с помощью удобного и простого подхода. Например, большинство современных смартфонов оснащены модулем распознавания отпечатков пальцев, что является надежным и экономичным методом аутентификации пользователя [6].

Методы аутентификации на основе физиологической биометрии демонстрируют высокую эффективность, точность и приемлемость для пользователей [12]. Однако все эти методы требуют от пользователя знания технологических особенностей, поскольку пользователь должен взаимодействовать с биометрическим датчиком и знать о процессе сбора биометрических данных. Подобно схемам аутентификации, основанным на знаниях, физиологические биометрические данные, например, по лицу, отпечатку пальца, окологлазной и радужной оболочке глаза, могут обеспечивать аутентификацию в точке входа и не обеспечивают неявной и прозрачной аутентификации.

Очевидно, что методы, основанные на знаниях и физиологических биометрических данных, успешны для проверки пользователей, но они не обеспечивают непрерывной и прозрачной аутентификации. Более того, физиологическая биометрия в основном зависит от аппаратного обеспечения. Поведенческая биометрия демонстрирует более высокий потенциал для удовлетворения всех требований к эффективной системе аутентификации. В дополнение ко всем преимуществам использования поведенческих биометрических данных, они являются подходящим решением для защиты от отказа пользователя [1] или в случае отсутствия законного пользователя разблокированного устройства. Эти мно-

гочисленные преимущества аутентификации на основе поведенческой биометрии оказались важными для принятия пользователями (описанный в [11] опрос показал, что 90 % участников исследования отдают предпочтение прозрачной аутентификации на основе поведенческой биометрии). Сегодня наблюдается значительный интерес к использованию различных поведенческих модальностей, таких как динамика нажатия клавиш, сенсорные жесты, движение, голос и т.д. для прозрачной аутентификации пользователей на мобильных устройствах. Наличие датчиков на современных мобильных устройствах сделало возможным работу фоновых приложений, предназначенных для моделирования поведения человека [9], аутентификации пользователя [5], распознавания активности и действий [6], мониторинга состояния здоровья [4].

Для биометрической аутентификации используется несколько модальностей, в том числе физиологическая биометрия (лицо, отпечаток пальца, радужная оболочка и т.д.) и поведенческая биометрия (динамика нажатия клавиш, сенсорные жесты, голос, движения и т.д.). Все эти способы становятся возможными благодаря встроенным мобильным датчикам, например, камере, микрофону, акселерометрам и гироскопам, которые участвуют в фазе регистрации и верификационной части процесса аутентификации. Такие датчики предоставляют достаточную информацию для точной и безопасной аутентификации [6]. Вопросы реализации «биометрии на ходу» рассмотрены в [4].

Существует два распространенных подхода к регистрации пользователей в системе аутентификации пользователей. Для простоты мы классифицируем методы регистрации на регистрацию на основе шаблона и регистрацию на основе модели. Для регистрации на основе шаблона пользователь отправляет несколько образцов, чтобы зарегистрировать шаблоны для будущего сравнения. Это достаточно популярный метод аутентификации с использованием физиологической биометрии, в которой признаки могут быть более устойчивыми к внутриклассовым вариациям, а также более отличительными и масштабируемыми для большой совокупности.

После регистрации шаблонов пользователей применяется основанный на сходстве метод для проверки пользователей на соответствие определенным пороговым значениям. Для улучшения качества важны надежность функций определения пользователя и обеспечение удаления статистических выбросов, а снижение избыточности факторов — для увеличения производительности. Кроме того, необходимо обеспечить безопасность и конфиденциальность шаблонов пользователей, как непосредственно во время самого процесса регистрации шаблона, но и во время хранения, извлечения и обработки для аутентификации пользователя.

При регистрации на основе модели биометрические данные пользователей собираются для обучения модели машинного обучения для аутентификации пользователя, где модель аутентификации решает, принадлежат ли входные данные законному пользователю. Общие подходы к машинному обучению используются для создания пользовательских моделей, включая сбор и предварительную обработку данных, извлечение и выбор признаков, а также моделирование. Наиболее эффективные методы включают в себя оценку признаков и процесс их отбора, чтобы выделить наиболее отличительные признаки среди большой совокупности. В последнее время подходы на основе моделей набирают успех для задачи аутентификации пользователя. Однако для эффективного внедрения необходимо решить несколько проблем, таких как размер собираемых данных, время обучения, размер модели и устойчивость к возможным атакам злоумышленников.

После регистрации пользователя система проверяет его подлинность на основе извлеченных признаков. Проверка может осуществляться в точке входа и непрерывно в течение сеанса использования. Для непрерывной аутентификации процесс проверки пользователя происходит периодически, чтобы сохранить доступ законному пользователю и запретить доступ мошенникам. Частота проверки должна быть тщательно подобрана, чтобы обеспечить достаточное количество и качество биометрических данных, а также сбалансировать потребление энергии. В зависимости от подхода к регистрации алгоритм аутентификации следует схеме, основанной на сходстве или вероятности, для проверки пользователя. Методы на основе сходства используются для измерения сходства входных данных по сравнению с сохраненным шаблоном для определенного пользователя. Традиционно проверка подразумевает совпадение заданных данных с сохраненным шаблоном с учетом допустимого порогового отклонения. Система аутентификации отвечает за предоставление доступа законному пользователю при предоставлении им биометрических данных, которые соответствуют предполагаемому шаблону с проверкой подобия выше заранее определенного порогового значения. Порог используется для учета ошибок и отклонений значений признаков, которые могут повлиять на считывание или вычисление биометрических данных.

Быстрое развитие мобильных технологий за последние годы увеличило производительность смартфонов в несколько раз. Вычислительные возможности мобильных устройств, использующих многоядерные процессоры, графические процессоры и гигабайты памяти, сопоставимы с возможностями обычных настольных компьютеров. Устройства аппаратного ускорения, доступные на большинстве платформ чипсетов смартфонов (например, Qualcomm, HiSilicon, MediaTek и Samsung), позволяют запускать на смартфонах слож-

ные приложения, выходящие далеко за рамки стандартных и встроенных функций телефона. Современные смартфоны оснащены различными датчиками, например, датчиками движения, датчиками окружающей среды и датчиками положения, которые могут обеспечить точное профилирование использования для повышения удобства работы пользователей. Хотя стандартные приложения сталкиваются с меньшим количеством проблем при таких возможностях технологий, существует множество требований к производительности и проблем, связанных с внедрением непрерывной аутентификации на основе поведения на смартфонах, особенно при использовании подходов машинного обучения.

Доступность преимуществ встроенных модулей ускорения обработки информации играет ключевую роль в разработке методов непрерывной аутентификации. Однако, несмотря на то что текущие вычислительные мощности и объем памяти смартфонов позволяют сопоставлять входные данные с моделью, этап регистрации признаков может быть сложной задачей и может потребовать этапа обучения на стороне сервера. Эффективная реализация метода аутентификации на основе поведенческих биометрических данных должна учитывать независимую от аппаратного и программного обеспечения работу и различия в сетевом подключении, чтобы обеспечить успешное внедрение системы.

Большинство встроенных методов аутентификации представлены на базовом уровне, поскольку непрерывная неявная аутентификация все еще развивается, чтобы соответствовать определенному уровню стандартов. Препятствием для массового производства встроенных возможностей аутентификации в смартфонах является то, что они должны соответствовать высоким стандартам безопасности (например, FAR 0,01 % в Европейском Союзе).

Разработанный с участием автора статьи способ непрерывной аутентификации пользователя многофункционального мобильного электронного устройства, учитывающий возможности современных технологий, описан в [16].

ЛИТЕРАТУРА

1. Kaspersky Lab has calculated how many times hackers have tried to steal passwords from Russians. URL: https://clck.ru/32kJ6s.
2. What is Multi-factor Authentication (MFA)? URL: https://clck.ru/32kJ8w.
3. Кузьминых Е.С., Маслова М.А. Анализ и сравнение биометрических способов идентификации личности человека // Научный результат. Информационные технологии. — 2021. — Т. 6. — № 4. — С. 13–19.
4. Девицына С.Н., Елецкая Т.А., Балабанова Т.Н., Гахова Н.Н. Разработка интеллектуальной системы биометрической идентификации пользователя // Научные ведомости Белгородского государственного университета. Серия: Экономика. Информатика. 2019. Т. 46. № 1. С. 148–160.
5. Fedotov A.S. Basic principles of implementing multi-factor authentication // 67th Scientific and Technical Conference of students, undergraduates and undergraduates, April 18–23, Minsk: collection of scientific papers: at 4 h. h. 4.
6. Маслова М.А. Анализ и определение рисков информационной безопасности // Научный результат. Информационные технологии. — 2019. — Т. 4. — № 1. — С. 31–37.
7. Troshkov A.M., Kondrashov A.V., Kondrashov Yu.V., Khlobystin N.S., Krylova L.A. Biometric characteristics of identity authentication and their protection system // Questions of defense technology. Series 16: Technical means of countering terrorism. Founders: Scientific and Production Association of Special Materials, FSUE «Scientific and Technical Center «Informtechnika» ISSN: 2306–1456.
8. Герасимов В.М., Маслова М.А. Возможные угрозы и атаки на систему голосовой идентификации пользователя // Научный результат. Информационные технологии. — 2022. — Т. 7. — № 1. — С. 32–37.
9. Bardaev S.E. Multifactorial biometric threshold cryptosystem // Izvestiya SFU. Technical sciences. Founders: Southern Federal University ISSN: 1999-9429eISSN: 2311–3103
10. Devitsyna S., Eletskaya T., Meshkov A.V. Developing facial recognition software to control access to campus facilities sbornike: CEUR Workshop Proceedings. 2. Ser. «InnoCSE 2019 — Proceedings of the 2nd Workshop on Innovative Approaches in Computer Science within Higher Education» 2019. P. 68–76.
11. Krotov A.V., Kutuzov A.V. Application of multi-factor authentication in order to protect EUT funds from unauthorized access // Modern scientific research and innovation. 2021. № 3.
12. Bogdanov D.S., Klyuev S.G. Classification and comparative analysis of multifactor authentication technologies in web applications // Modeling, optimization and information technology. Founders: Voronezh Institute of High Technologies eISSN: 2310–6018
13. Types Of Biometrics: A Complete Guide. URL: https://clck.ru/32knZ3.
14. Надейкина В.С., Лагуткина Т.В. АНАЛИЗ СПОСОБОВ РЕАЛИЗАЦИИ СИСТЕМЫ МНОГОФАКТОРНОЙ АУТЕНТИФИКАЦИИ //Научный результат. Информационные технологии. — 2022. — Т. 7. — №. 4. — С. 59–66.
15. Маслова М.А., Костиков В.А. Использование системы голосовой идентификации в качестве дополнительной защиты пользователя // Современные проблемы радиоэлектроники и телекоммуникаций. — 2021. — № 4. — С. 223.
16. Бугаков А.И., Бугаков И.А., Царьков А.Н., Шульга М.М. Способ защиты электронного многофункционального мобильного устройства от несанкционированного доступа. Заявка на выдачу патента № 2022126590/07(058037) от 11.10.2022. Заявитель: АНО «Институт инженерной физики».

Журнал «Современная наука: актуальные проблемы теории и практики»