DOI 10.51582/interconf.21-22.05.2021.031

Мазниченко Наталья Ивановна
старший преподаватель кафедры криминалистики
Национальный юридический университет имени Ярослава Мудрого,
Украина

ИДЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ МОБИЛЬНЫХ УСТРОЙСТВ С ИСПОЛЬЗОВАНИЕМ ДИНАМИКИ НАБОРА ПАРОЛЬНОЙ ФРАЗЫ

Аннотация. *Текущая безопасность мобильных устройств часто ограничивается персональным идентификационным номером (PIN), методом, основанным на секретных знаниях, который исторически продемонстрировал свою неэффективную защиту от неправомерного использования. В этом исследовании предлагается использовать двухфакторную идентификацию в качестве усовершенствованного метода идентификации для мобильных устройств с сенсорным экраном. На основе анализа сделан вывод, что за счет использования секретных данных и анализа нажатия клавиш будет обеспечен более надежный механизм ограничения доступа к мобильным устройствам.*
Ключевые слова: *информационная безопасность, идентификация пользователя, биометрическая идентификация, динамика нажатия клавиш.*

Постановка проблемы. В современном мире технологии претерпели столь значительные изменения, что мобильные устройства приобрели функциональные возможности, свойственные компьютерным системам. По мере того, как смартфоны развиваются как в аппаратном, так и в программном обеспечении, их функции стали разнообразнее: осуществление финансовых операций, доступ к онлайн-банкингу, способность хранить важную конфиденциальную информацию, что делает их целью для злоумышленников. По мере того, как все больше личной и конфиденциальной информации хранится на смартфонах, риск утечки информации становится все более серьезной проблемой. Наиболее распространенный механизм решения этой проблемы − идентификация. Цель идентификации − гарантировать, что

доступ предоставляется только уполномоченному лицу. Однако механизмы идентификации могут различаться как по сложности, так и по стоимости.

Самый распространенный метод идентификации для мобильных телефонов на сегодняшний день − это использование PIN-кода (персонального идентификационного номера), который имеет ограничения, как с точки зрения конечного пользователя, так и с технологической точки зрения. Следовательно, существует потребность в ненавязчивой и более надежной методике проверки пользователей. Один из потенциальных подходов − использование биометрических характеристик, которые основаны не на знаниях пользователя, а на самом пользователе. Для обеспечения дополнительного уровня безопасности можно предложить использовать исследование динамики нажатия клавиш во время ввода пароля или PIN-кода, позволяющее анализировать ритм набора текста пользователем.

Анализ литературы. Одно из первых исследований динамики нажатия клавиш как метода идентификации пользователя было проведено в 1980 году [1]. Следует отметить, что в последние годы в связи с актуальностью проблемы информационной безопасности в сфере цифровых технологий, интерес к исследованиям возможности использования данной динамической характеристики возрос, о чем свидетельствует значительное количество публикаций по данной теме. Но так же необходимо отметить, что значительная часть исследований касается клавиатур компьютерных систем. Учитывая повсеместное распространение и возросший функционал современных мобильных телефонов, появляется все больше работ, посвященных исследованиям динамики работы с сенсорными и программными клавиатурами на мобильных устройствах для идентификации пользователя [2-8].

Исследования публикаций относительно использования динамики ввода парольной фразы для мобильных устройств не дают четкого ответа на вопрос, какой из представленных методов дает лучшие показатели распознавания пользователя. Также следует отметить, что в представленных работах, к сожалению, не рассматривались форм-фактор и вычислительные возможности устройства, зачастую устройство использовалось только для

сбора образцов, а затем для анализа образцов использовались компьютерные системы.

Цель статьи. Рассмотрим использование динамики нажатия клавиш в качестве дополнительного фактора для идентификации пользователей мобильных телефонов при вводе пароля или PIN-кода. Проанализируем возможность, целесообразность, эффективность использования такой идентификационной характеристики для повышения надежности защиты мобильных устройств.

Материалы исследования. В эпоху интеллектуальных технологий количество пользователей смартфонов растет с каждым годом, что, в свою очередь, потребовало применения дополнительных мер безопасности по отношению к информации, которая хранится на данных устройствах. Чаще всего для ограничения доступа к мобильным телефонам используются либо PIN-код либо графический пароль, хотя в настоящее время все большее распространение получают такие технологии как сканирование отпечатков пальцев, использование изображения лица или других биометрических характеристик. Однако следует отметить, что наиболее распространенным на сегодняшний день является именно PIN-код как механизм ограничения доступа к мобильным устройствам, который не может обеспечить адекватной защиты от современных угроз. Поэтому целесообразно обратить внимание на другие способы идентификации.

Идентификация может быть достигнута с использованием одного из трех подходов [9, с. 216]. Первый − использовать то, что знает пользователь (PIN-код относится к этой категории, как и пароль). Вторая категория использует то, что есть у пользователя, например токен, различные карты. Наконец, третья категория использует то, кем является пользователь. Эта категория широко известна как биометрия, в ней используются некоторые индивидуальные характеристики пользователя. Биометрические характеристики можно разделить на статические и динамические [9, с. 221]. Статические (физиологические) включают такие атрибуты, как сетчатка глаза, отпечатки пальцев, геометрия руки, изображение лица и т. д. Другой вариант

биометрической идентификации − это поведенческая биометрия, которая использует такие динамические характеристики как подпись, голос, походка, особенности работы с клавиатурой и т. д.

Биометрическая идентификация − удобный и точный метод идентификации. Одним из вариантов биометрической идентификации является анализ нажатия клавиш при работе с цифровыми устройствами.

Подход, предлагаемый в этой статье, заключается в использовании комбинации секретных знаний (пароля или PIN –кода) и биометрии (анализ динамики нажатия клавиш при вводе парольной фразы). В данном случае, технология, основанная на секретных знаниях, будет использоваться как обычно, но также будет анализироваться ритм нажатия клавиш для обеспечения дополнительной проверки.

Преимущества идентификации пользователя на основе анализа динамики нажатия клавиш:

− уникальность: есть возможность измерять временные данные с точностью до наносекунд для событий нажатия клавиш, чтобы точно идентифицировать пользователя;

– низкие затраты на внедрение и использование: распознавание динамики нажатия клавиш не требует дополнительного оборудования и может быть полностью реализовано с помощью программного обеспечения;

− скрытность: пользователь может не знать о том, что в некоторых системах реализован дополнительный уровень идентификации с использованием динамики нажатия клавиш;

− надежность: использование динамики нажатия клавиш в схеме идентификации пароля может повысить ее надежность.

Использование динамики нажатия клавиш на мобильных устройствах имеет определенные особенности в сравнении с обычными клавиатурами, которые используются в персональных компьютерах:

– использование меньшего количества пальцев (чаще всего используются только два больших пальца и один указательный);

– в компьютерных системах со сменой клавиатуры шаблон ввода символов пользователем может отличаться, а в мобильных устройствах с сенсорным экраном это не так.

Следует отметить, что сенсорный экран или программная клавиатура на смартфоне предполагает значительно больше проблем для анализа нажатия клавиш в сравнении с аппаратной клавиатурой. Поскольку аппаратные клавиатуры имеют более или менее устоявшуюся форму, компоновку и используются людьми на протяжении значительного периода, большинство людей гораздо лучше знакомы и умеют обращаться с ними, чем с сенсорными клавиатурами. Небольшой форм-фактор смартфона, значительные различия в размере клавиатуры и ее раскладке, а также проблемы, возникающие у некоторых людей от использования программных клавиатур из-за отсутствия физической обратной связи, которую они получали бы от аппаратной клавиатуры, − все это в совокупности может привести к разительным отличиям работы с сенсорными или программными клавиатурами в сравнении с аппаратными клавиатурами.

Общий процесс для систем идентификации на основе нажатия клавиш требует следующих двух этапов [10, с. 142]: регистрации (обучения) и непосредственно идентификации.

На этапе обучения пользователь вводит парольную фразу (в некоторых случаях требуется повторять это действие несколько раз). При этом рассчитываются и запоминаются эталонные характеристики данного пользователя (создается эталонный шаблон пользователя). На этапе идентификации пользователь, претендующий на доступ, вводит парольную фразу, для которой рассчитываются те же самые характеристики, которые сравниваются с эталонными. В зависимости от результата сравнения пользователь либо получает доступ к защищаемому устройству либо нет.

В процессе ввода парольной фразы определяется, какая клавиша была нажата, время удержания клавиши, время, когда она была отпущена. И так для каждого символа парольной фразы. Иногда могут использоваться и другие характеристики: время между нажатиями двух последовательных клавиш,

сила нажатия на клавиши, частота ошибок и другие. Далее эти временные характеристики используются для создания индивидуального шаблона пользователя.

Современные мобильные устройства оснащены рядом сенсоров, которые могут использоваться мобильными приложениями. Так, API Android предоставляет приложениям возможность использовать различные датчики, такие как гравитация, давление воздуха, влажность, микрофон, камера, акселерометр, приближение, свет, гироскоп. Основное внимание уделяется датчикам движения, то есть гироскопу и акселерометру. Акселерометр вычисляет ускорение мобильных устройств по осям X (поперечная), Y (продольная) и Z (вертикальная). Приложения могут получить доступ к значениям ускорения, оцениваемым акселерометром. Гироскоп, в свою очередь, измеряет ориентацию (угол) устройства вокруг каждой из трех физических осей. Набор из трех углов, задающих ориентацию телефона в трехмерном пространстве, позволяет определить, в каком месте пользователь нажал на экран. Каждая клавиша имеет уникальную картину изменений углов по трем осям, которые могут быть идентифицированы. Приложения могут рассчитывать значения скорости вращения (радиан/секунду), ориентации (угла) и вектора вращения (ориентация устройства как комбинация оси и угла), заданных гироскопом [11, с. 95]. Таким образом, гироскоп и акселерометр могут широко использоваться в приложениях, где требуется характеристика поведения, например, для определения местоположения или нажатия клавиш на основе датчиков. В данном случае динамика датчика может предоставить очень важную информацию для точного распознавания действий, выполняемых пользователем на мобильном устройстве.

Для реализации процесса распознавания пользователя в системах идентификации используют классификатор, основанный на одном из следующих математических подходов [12, с. 3]: статистические методы, нейронные сети, методы распознавания образов, комбинированные.

Алгоритмы, основанные на статистике, имеют невысокие требования к производительности, что важно для мобильной платформы. Нейросетевые

алгоритмы, скорее всего, будет иметь высокие требования к обработке, но в данном случае, показатели точности идентификации обычно лучше. Преимущество использования нейронных сетей заключается в том, что они гибки для различных типов наборов данных. Кроме того, можно одновременно рассматривать большое количество наборов данных. К тому же, нейронную сеть можно обучить специально для конкретного пользователя.

Любая биометрическая идентификация имеет недостаток, заключающийся в том, что некоторые пользователи ошибочно принимаются (коэффициент ложного принятия, известный как FAR), а некоторые − ошибочно отклоняются (ложное отклонение, известное как FRR) [10, с. 142]. Это означает, что злоумышленник, пытающийся получить доступ к системе, может быть принят, в то время как действительный пользователь может быть отклонен. Для получения лучших результатов частота ошибок должна быть как можно ниже, а также должна быть сбалансирована для особых случаев, поскольку оба значения не могут быть равны нулю одновременно.

Иногда вместо FRR и FAR оценивается EER (равная частота ошибок). Это происходит, когда FRR и FAR эквивалентны. Основная задача − найти правильное пороговое значение для сравнения шаблона претендента на доступ и эталонного шаблона зарегистрированного пользователя. Для некоторых систем требуется низкий FAR (высокий порог), чтобы злоумышленник не мог проникнуть в систему. Фактически, это лучшее решение для создания высокозащищенных систем.

На сегодняшний день представлено достаточное количество разработок в сфере идентификации пользователя по динамике набора пароля или PIN –кода для мобильных устройств с сенсорным экраном. Однако следует отметить, что большинство научных работ по данной теме, являются независимыми исследованиями, каждое из которых основано на определенном количестве образцов, собранных от уникальных наборов пользователей. Исследователи собирали эти образцы с помощью разных методов и широко варьировались в измеряемых данных, количестве входных данных, необходимых для обучения системы и идентификации пользователей, количестве испытуемых и

разнообразии этих испытуемых, условиях тестирования, мобильных устройствах. Такая неоднородность усложняет процесс сравнения разных исследований. Если прибавить к этому разнообразие подходов к классификации пользователей и применению этих технологий в разных областях, задача становится еще сложнее. Именно от решения данных проблем будет зависеть популярность и востребованность данной технологии у пользователей мобильных устройств.

По поводу количества и информативности параметров динамики нажатия клавиш, используемых при построении системы идентификации, мнения разных авторов также различаются. Следует отметить, что большинство авторов используют только две временные характеристики: нажатие (удержание) клавиши и интервалы между нажатиями двух последовательных клавиш. Некоторые авторы считают, что сила нажатия пальца во время набора символа является лучшим индикатором для идентификации пользователей по сравнению с такими характеристиками, как время удержания клавиши и пауза между нажатиями клавиш. А некоторые авторы утверждают, что сочетание временных характеристик с силой нажатия дает лучшие результаты по сравнению с их использованием отдельно.

Сравнить и оценить результаты исследований систем идентификации пользователей мобильных устройств по динамике набора парольной фразы по разным показателям можно с использованием таблиц, представленных в работе [12, с. 4]. Для разных исследований можно узнать: какие информативные параметры использовались; методы, которые использовались для классификации пользователей; разновидность парольной фразы (PIN- код, произвольные символы, только цифры); длина парольной фразы; полученные значения EER, FAR, FRR; полученная точность идентификации; количество пользователей, которые принимали участие в экспериментах; мобильные устройства, которые использовались в экспериментах; информацию об исправлениях при наборе; собранное количество образцов. Такая статистическая информация очень полезна для того, чтобы было легче определиться с выбором.

Выводы. В данной статье были рассмотрены и исследованы некоторые существующие системы идентификации пользователей по динамике набора парольной фразы или PIN-кода для мобильных устройств с сенсорным экраном. Анализ данных систем позволяет сделать вывод о том, что комбинация двух факторов идентификации (PIN-кода/пароля и анализа динамики его ввода) обеспечит более высокий уровень защиты устройства от неправомерного использования нелегитимным пользователем. Даже если злоумышленник каким-либо способом узнает PIN-код, дополнительной линией защиты будет требование вводить его с использованием определенного ритма.

Учитывая тот факт, что PIN-код, используемый для ограничения доступа к мобильным телефонам, имеет весьма ограниченное (небольшое) количество символов, представляется целесообразным использовать специфический (заранее продуманный) ритм набора символов, что обеспечит более точный процесс идентификации пользователя.

Учитывая тенденции развития современных мобильных устройств можно с уверенностью утверждать, что технология идентификации пользователей таких устройств по ритму ввода парольной фразы или PIN-кода имеет большой потенциал и будет востребованной благодаря следующим преимуществам: простота и удобство использования с учетом привычных для пользователя процедур ввода пароля; отсутствие потребности в приобретении дополнительных устройств из-за использования встроенной сенсорной клавиатуры.

Список источников:

1. R. S. Gaines, W. Lisowski, S. J. Press, N. Shapiro. Authentication by keystroke timing: some preliminary results. Technical Report № RAND-R-2526-NNSF. Rand Corporation, Santa Monica, CA, 1980. 51 p.
2. Chang TY, Tsai CJ, Lin JH. A graphical-based password keystroke dynamic authentication system for touch screen handheld mobile devices. *The Journal of Systems and Software*. 2012. Volume 85. Issue 5. Pp.1157-1165.
3. N. Zheng, K. Bai, H. Huang, H. Wang. You are how you touch: user verification on smartphones via tapping behaviors. *Network Protocols (ICNP ’14)*: Proceedings of the IEEE

22nd International Conference. (October 2014). North Carolina, NC, USA, 2014. Pp. 221–232.

4. M. Antal, L. Z. Szabŏ. Keystroke Dynamics on Android Platform. *Procedia Technology*. 2015. Vol. 19. Pp. 820–826.
5. S. Dhage, P. Kundra, A. Kanchan, and P. Kap. Mobile authentication using keystroke dynamics. *Information and Computing Technology, ICCICT '15*: Proceedings of the International Conference on Communication. (January 2015). Mumbai, India, 2015. Pp. 15–95.
6. T.-Y. Chang, C.-J. Tsai, W.-J. Tsai, C.-C. Peng, H.-S. Wu. A changeable personal identification number-based keystroke dynamics authentication system on smart phones. *Security and Communication Networks*. 2016. Vol. 9. № 15. Pp. 2674–2685.
7. Довгаль В.А. Особенности захвата параметров клавиатурного почерка. *Вестник АГУ*. 2017. Выпуск 2 (201). С. 102-108.
8. P. S. Teh, N. Zhang, A. B. J. Teoh, K. Chen. TDAS: a touch dynamics based multi-factor authentication solution for mobile devices. *International Journal of Pervasive Computing and Communications*. 2016. Vol. 12. № 1. Pp. 127–153.
9. Кошева Н. А., Мазниченко Н. І. Ідентифікація користувачів інформаційно-комп'ютерних систем: аналіз і прогнозування підходів. *Системи обробки інформації*. 2013. Випуск 6 (113). С. 215-223.
10. Кошевая Н.А., Мазниченко Н.И. Подход к повышению надежности идентификации пользователей компьютерных систем по динамике написания паролей. *Системи обробки інформації: збірник наукових праць*. 2014. Вип. 6 (122). С. 140-146.
11. C. Giuffrida, K. Majdanik, M. Conti, H. Bos. I sensed it was you: authenticating mobile users with sensor-enhanced keystroke dynamics. *Detection of Intrusions and Malware, and Vulnerability Assessment:* Proceedings of the 11th International Conference. (July 2014). Cham, Switzerland, 2014. Vol. 8550. Pp. 92–111.
12. Baljit Singh Saini, Navdeep Kaur, Kamaljit Singh Bhatia. Keystroke Dynamics for Mobile Phones: A Survey. *Indian Journal of Science and Technology*. 2016. Vol 9(6). Pp. 1-8.