УДК 621. 321.*11*

Д.Ш.ОСМОНАЛИЕВ, И.К.МАНАПБАЕВ.,
А.С.ХМИЛЕВСКИЙ, Ж.Р.ОСМОНОВА
E-mail: ksucta@élcat.kg

БИОМЕТРИЧЕСКАЯ АУТЕНТИФИКАЦИЯ МОБИЛЬНЫХ ПОЛЬЗОВАТЕЛЕЙ

Бул эмгекте мобилдүү телефондогу маалыматтарга жетүү үчүн клавиатуралык жазма боюнча аутентификациалоону колдонууну көрсөтүүчү усулдар каралган. Учурдагы мобилдүү телефонлорду аутентификациалоо усулдарына талдоо жүргүзүлгөн. Сунушталган усулдун маңызы ачылып, тажрыйбалардын жыйынтыктары көрсөтүлгөн.

Изилдөөлөрдүн жана тажрыйбалардын жүрүшүндө иштелип чыккан усул уюлдук операторлордун карларларында маалыматка жетүүнү башкаруу үчүн колдонулушу мүмкүн.

В данной работе рассматриваются методы, демонстрирующие применение аутентификации по клавиатурному почерку для управления доступом к информации на мобильных телефонах. Проведен обзор существующих методов аутентификации мобильных телефонов. Раскрыта сущность предлагаемого метода, и приведены результаты экспериментов.

Разработанный в ходе исследований и экспериментов метод может быть использован на практике для управления доступом абонентов сотовых операторов.

In the given job methods showing application autentification keyboard handwriting for management of access to the information on mobile phones are considered. The review of existing methods autentification mobile phones is spent. The essence of an offered method is opened, and results of experiments are resulted.

Developed during researches and experiments the method can be used in practice for management of access of subscribers of cellular operators.

В современном мире мобильные устройства, такие как мобильные телефоны, смартфоны, коммуникаторы в значительной мере перенимают функции персонального компьютера. Часто мобильные телефоны снабжаются программным обеспечением для хранения личной и деловой информации (так называемые электронные бумажники, electronic wallets), выполнения банковских транзакций (mobile banking software), покупок товаров и услуг и т.д. Стоимость информации, находящейся в мобильном телефоне,

становится весьма высокой. Поэтому мобильный телефон становится привлекательной целью злоумышленников – компактное устройство, носимое в одежде, которое может быть легко похищено. При этом защита самого абонентского устройства и услуг, предоставляемых через это устройство, в настоящее время осуществляется через 4-значный PIN-код. Многие эксперты отмечают недостатки подобной защиты /1, 2/, основная из которых – аутентификация не личности пользователя, а проверка знания некоторой информации, в данном случае пароля или PIN-кода. Биометрическая аутентификация может стать эффективным решением данной проблемы. В настоящее время работы в этом направлении ведутся различными производителями мобильных телефонов. Например, в августе 2003 года фирма NTT DoCoMo представила на рынок мобильный телефон F505i со встроенным считывателем отпечатков пальцев. Однако внедрение мобильных биометрических устройств производится в основном японскими операторами связи и производителями телефонов, такими как NTT DoCoMo для своих сетей формата CDMA и W-CDMA. Единственным GSM-телефоном со встроенным считывателем отпечатков пальцев в настоящее время является мобильный телефон Pantech GI100, представленный в 2004 году корейской компанией Pantech. Другие производители GSM-телефонов, например, Nokia, Siemens, LG в настоящее время только планируют выпуск телефонов с возможностями биометрической аутентификации.

В данных условиях универсальным решением может стать внедрение программных средств биометрической аутентификации пользователя в мобильном телефоне. Программные решения обеспечивают быстрое внедрение, возможность постоянного обновления алгоритмов и низкую стоимость.

1. Обзор методов биометрической аутентификации для мобильных устройств

Возможные методы биометрической аутентификации для мобильных устройств определяются возможностями подключения к мобильному устройству биометрических сенсоров, сканеров отпечатков, систем ввода изображения и т.д. С учетом приведенной информации о комплектации мобильных устройств сканерами отпечатков можно считать, что сканирование отпечатков пальцев не станет в ближайшее время распространенным средством мобильной аутентификации. Еще в большей мере трудно ожидать распространения таких методов аутентификации, как сканирование ладони, сетчатки глаза и т.д., вследствие значительных габаритов считывателя. В работе /3/ приводятся следующие возможные методы биометрической аутентификации мобильного пользователя (рис. 1).

Рис. 1. Возможные методы биометрической аутентификации мобильных пользователей (на основе /3/)

Можно привести следующие соображения о применимости некоторых видов биометрической аутентификации:

1. Распознавание лица. Большинство современных мобильных устройств среднего класса снабжены фото- и видеокамерами. Однако существуют сомнения в эргономичности и производительности данного метода. В большинстве телефонов камеры расположены так, что осуществить автопортретную съемку очень сложно. Для захвата изображения лица пользователь должен держать телефон на расстоянии вытянутой руки. С учетом того факта, что в таком положении очень сложно зафиксировать руку, изображение лица будет получено с искажениями. Кроме того, необходимо учитывать, что операции с изображениями обычно являются весьма ресурсоемкими.

2. Распознавание радужной оболочки глаза. Очевидно, что соображения относительно распознавания лица актуальны и в данном случае. Кроме того, распознавание оболочки глаза требует высокой освещенности помещения.

3. Динамика использования сервисов. Очевидно, что данная методика может использоваться только для мониторинга использования устройства, а не для аутентификации пользователя. Таким образом, динамика использования сервисов поможет определить злоумышленника и отключить его от сервисов, но не защитить персональную информацию пользователя.

4. Распознавание подписи. Очевидно, что метод применим только для устройств с сенсорным экраном. Процент мобильных телефонов и смартфонов с сенсорным экраном в настоящее время не велик, хотя среди PDA и коммуникаторов подавляющее большинство снабжено подобными экранами. Кроме того, метод может быть реализован как статически, так и динамически, что повышает его безопасность.

5. Динамика клавиатурного почерка. По нашему мнению, это один из наиболее эффективных методов биометрической аутентификации мобильных пользователей. Большинство мобильных телефонов снабжено клавиатурой. Метод также может использоваться для устройств с сенсорным экраном (виртуальная клавиатура). Пароль, от которого зависит динамика набора, является сменяемым секретным параметром. Оценка клавиатурного почерка может быть реализована быстрыми статистическими алгоритмами.

6. Голосовая аутентификация. Этот вид аутентификации также является весьма перспективным. Все существующие в настоящее время мобильные устройства снабжены звуковыми подсистемами. Голосовая аутентификация не требует специального расположения мобильного устройства в пространстве. Методика голосовой аутентификации может быть как текстонезависимой, так и зависящей от текста. Однако голосовая аутентификация сильно зависит от состояния среды и весьма требовательна к вычислительным ресурсам.

Таким образом, аутентификация по динамике клавиатурного почерка позволит разработать наиболее простую и эффективную систему биометрической аутентификации для мобильных устройств. Для подтверждения этой гипотезы в данной работе предлагается насколько возможно простой и быстрый алгоритм аутентификации пользователя по динамике набора пароля.

Необходимо отметить, что аутентификация по динамике набора на клавиатуре мобильного телефона должна отличаться от аутентификации по динамике набора на клавиатуре настольного компьютера или ноутбука. Приведем факторы, которые, по нашему мнению, могут оказывать влияние на технику аутентификации по клавиатурному почерку:

1. Физиологические особенности руки. На клавиатурный почерк влияют как размер и форма руки и пальцев (в частности, людям с большими пальцами сложнее выполнять набор на клавиатуре телефона), так и физиологическое строение рук, в том числе возможные переломы, травмы и т.д.

2. Размер и форма телефона. В настоящее время производители выпускают телефоны с различными форм-факторами и размерами. Размер и форма телефона, в частности, размер и форма клавиш оказывают значительное влияние на клавиатурный набор.

3. Способ удержания мобильного телефона. У каждого пользователя, очевидно, формируется свой стиль удержания телефона. Способ удержания телефона также формирует клавиатурный почерк. Важным фактором является, удерживает ли пользователь телефон в левой или в правой руке.

4. Набираемый текст. Текст, который набирает пользователь, также оказывает влияние на скорость набора. Это фактор актуален как для клавиатур настольных компьютеров, так и для мобильных телефонов.

Важным вопросом является – насколько данные факторы влияют на динамику набора и позволяют точно определить пользователя. Работ по аутентификации по клавиатурному почерку на мобильном устройстве крайне мало. Одна из наиболее интересных работ на данную тему выполнена Н.Л. Кларком, С.М. Фарнелом и др. (N.L.Clarke, S.M.Furnell, e.t.c) /4/. Авторы исследуют возможность распознавания пользователя по набору PIN-кодов, произвольных телефонных номеров (10/11 символов + клавиша посыла вызова) и фиксированных телефонных номеров (10/11 символов + клавиша посыла вызова). В данной работе используется задержка между нажатиями клавиш. В качестве решающего правила используется сеть прямого распространения (многослойный персептрон). Авторы указывают, что наилучшие результаты для распознавания PIN-кодов были получены на многослойных персептронах, у которых 4 входных нейрона, 8 нейронов в первом и втором скрытом слое и один нейрон в выходном слое, наилучшие результаты для распознавания телефонных номеров получены на персептронах, у которых 11 входных нейронов, 22 нейрона в первом и втором скрытом слое, 1 нейрон в выходном слое. В ходе экспериментов исследованы ошибки FAR, FRR и ERR и получены результаты, приведенные в табл. 1 /4/. К сожалению, авторы не сообщают размер обучающей выборки и время обучения. Однако в экспериментах, проведенных в рамках данной работы, нейронные сети с подобной конфигурацией обучались около 1,5 и 5 минут соответственно на PC AMD Athlon XP 1800+ и RAM 512 Мб, что, очевидно, приведет к неприемлемо большому времени обучения на маломощных процессорах мобильного телефона.

Таблица 1

Результаты аутентификации (по [4])

Показатели	FAR (%)	FRR (%)	EER (%)
PIN- код	18,1	12,5	15
Произвольные номера	36,3	24,3	32
Фиксированные номера	16	15	15

Мы полагаем, что нейронные сети обеспечивают не самое лучшее решение задач аутентификации мобильного пользователя вследствие значительного времени обучения и требований к памяти. В данной работе предлагается метод, основанный на построении

быстрой и простой статистической модели распределения времени задержки нажатия клавиш при наборе заданного пароля.

1. Предлагаемый метод.

Метод основан на построении статистической модели, описывающей закономерности распределения времени между нажатиями клавиш при наборе заданного пароля. Как любой биометрический метод, разработанный метод требует предварительной настройки – регистрации пользователей.

Можно представить регистрацию пользователя следующей последовательностью действий:

1. Установить число повторов N=3, длина пароля K=8.

2. Создать вектор дисперсий $\bar{\sigma} = \{\sigma_1 .. \sigma_{K-1}\}$.

3. Повторить ввод регистрируемого пароля N раз. Получить $\bar{f}_i, i = [1..N]$ – вектор задержек между нажатиями клавиш. Каждый вектор $\bar{f}_i = \{f^i{}_1 ... f^i{}_{K-1}\}$.

4. Создать векторы кумулятивных сумм $\bar{\varphi}_i = \bar{f}_i, i = [1..N]$ и кумулятивных значений $\Sigma_i = 1, i = [1..N]$.

5. Создать шаблон, содержащий $\bar{f}_i, i = [1..N]$, $\bar{\sigma}$, $\bar{\varphi}_i$ и $\bar{\Sigma}$.

После настройки системы можно выполнять аутентификацию пользователей:

1. Ввести проверяемый пароль. Получить $\bar{f}' = \{f_1 ... f_{K-1}\}$ – вектор задержек между нажатиями клавиш аутентифицируемого пользователя.

$$\beta^i{}_j = \begin{cases} 1, & f^i{}_j - \sigma_j \le f_j{}' \le f^i{}_j + \sigma_j \\ 0, & \textit{иначе} \end{cases}$$

2. Создать вектор ошибок для всех $i = [1..N]$, $j = [1..K-]$.

3. Вычислить $\chi_i = \sum_j \beta^i{}_j$, $i = [1..N]$, $j = [1..K-]$.

4. Если $\chi_{\min} = \min(\chi_i) \le 5$, $i = [1..N]$, то пользователь прошел аутентификацию, иначе – нет.

5. Если на шаге 4, установлено, что пользователь прошел аутентификацию, то $I_{\min} = \min \arg(\chi_i)$; $\bar{\varphi}_{I_{\min}} = \bar{\varphi}_{I_{\min}} + \bar{f}'$, $\Sigma_{I_{\min}} = \Sigma_{I_{\min}} + 1$, $i = [1..N]$.

Вычисляется новое $\bar{f}_{I_{\min}} = \frac{\varphi_{I_{\min}}}{\Sigma_{I_{\min}}}, i = [1..N]$.

Таким образом, в данной модели можно указать несколько ключевых моментов:

1. Последовательность задержек нажатий клавиш пароля рассматривается как

набор независимых одномерных величин и анализируется отдельно. Отдельный анализ компонент обеспечивает большую устойчивость к ошибкам набора. Например, рассмотрим случай, когда пользователь допускает значительную ошибку в наборе одного символа. При оценке последовательность задержек нажатий клавиш как точки в многомерном пространстве ошибка в одной компоненте приведет к увеличению расстояния между шаблоном и проверяемым набором. При этом невозможно оценить, явилось это следствием небольших отклонений в каждой из задержек (клавиатурный почерк незарегистрированного пользователя) или сильного отклонения в одной из задержек (ошибки зарегистрированного пользователя).

2. Разные реализации клавиатурного пароля не приводятся к одному нормальному распределению, а рассматриваются как несколько ($N = 3$, в приведенном алгоритме 3) распределений с фиксированной дисперсией. Такое предположение позволит более точно аппроксимировать экспериментальное распределение.

3. В процессе аутентификации мы уточняем распределения, полученные на этапе регистрации. Уточнение (адаптация) распределений позволит увеличить точность аутентификации со временем.

Предложенный алгоритм является основой для системы биометрической аутентификации и распределения доступа. Система представлена на рис. 2. На рисунке видно, что система выполняет параллельную проверку пароля и динамики набора.

В дальнейшем при обсуждении экспериментальных результатов будут оцениваться ошибки первого и второго рода, присущие только биометрической компоненте.

2. Реализация и эксперименты

Для проверки работоспособности нашего алгоритма мы провели экспериментальные исследования. Для того чтобы обеспечить корректные оценки, недостаточно получить модельные данные на персональном компьютере, поскольку характеристика клавиатурного почерка клавиатуры персонального компьютера отличается от характеристик мобильных телефонов. Вследствие этого система была реализована в виде приложения Java для мобильного телефона (мидлета). Приложение разработано на основе технологии J2ME для устройств с MIDP 1.0. Это наиболее распространенный профиль Java для мобильных устройств, поддерживаемый подавляющим большинством мобильных телефонов.

Программа обеспечивает хранение персональной информации (электронный бумажник) с аутентификацией пользователя по клавиатурному почерку. Программа

позволяет добавлять биометрические профили пользователей, удалять профили пользователей, проводить собственно биометрическую аутентификацию при входе в программу, а также добавлять, редактировать и удалять деловые записи. На рис. 3 представлен экран регистрации нового пользователя. На рис. 4 показан экран аутентификации пользователя при входе в приложение.

В экспериментах участвовало 10 человек, каждый из которых был зарегистрирован и авторизован не менее 20 раз.

В табл. 2 представлены основные характеристики разработанного макета системы, полученные в результате лабораторного тестирования.

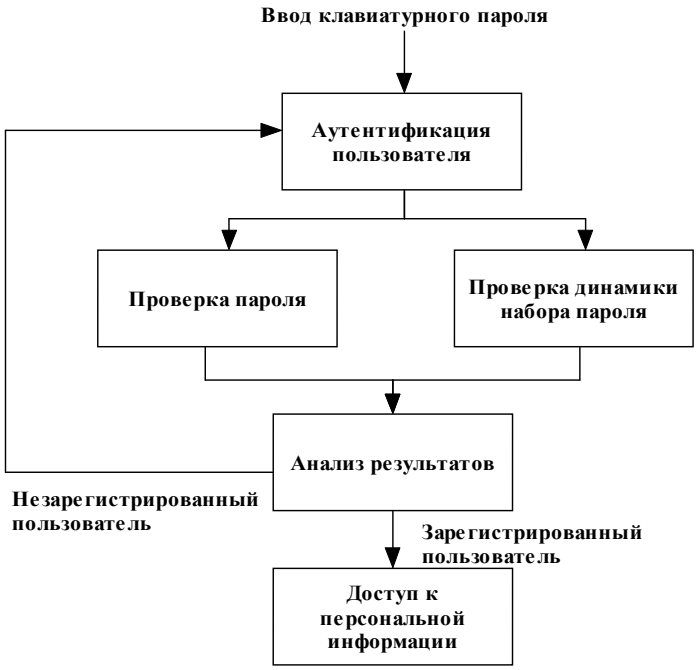

Рис. 2. Общая схема функционирования системы биометрической аутентификации по клавиатурному почерку

Поскольку клавиатурный почерк, как и многие другие биометрические характеристики, может быть сымитирован, то важным фактором является такая характеристика, как вероятность подбора пароля. Необходимо отметить, что в данном случае у злоумышленника есть подобная возможность. В экспериментах злоумышленник, не видя примера набора пароля зарегистрированным пользователем, тем не менее подбирал темп набора с 5–7 попытки.

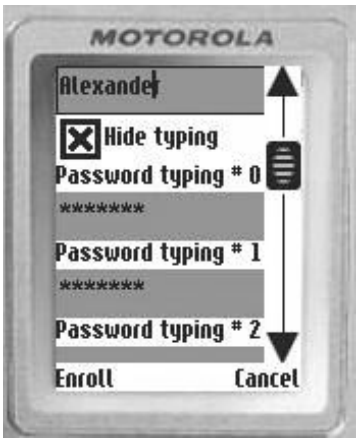

Рис. 3. Экран регистрации нового пользователя

Рис. 4. Экран аутентификации

Таблица 2

Основные характеристики биометрической аутентификации по клавиатурному почерку

Характеристика	Значение
Время регистрации одного пользователя	около 3 секунд
Время аутентификации одного пользователя	менее 0,5 секунды
Вероятность ложного отказа	15 %
Вероятность ложного допуска	5 %

Для предотвращения направленного подбора темпа набора предлагается использовать технологию так называемого «умного набора». В данном случае пользователь опирается не на естественный темп набора, а на разделение пароля на группы. Например, пароль может быть представлен в виде следующих групп: 782 45 6 12. Тогда при наборе групп цифр 782, 45, 12 время между нажатиями клавиш будет определяться клавиатурным почерком пользователя. Время между наборами групп будет зависеть как от желания пользователя, так и от клавиатурного набора. Может возникнуть соображение о том, что техника «умного набора» выводит применяемый в данной работе

клавиатурный почерк из числа биометрических методов, поскольку использует не поведенческие или физиологические характеристики, а осознанное действие пользователя по разбиению на группы набора цифр. Однако необходимо учитывать, что разбиение на группы показывает только точки увеличения задержек, сами задержки определяются физиологическими параметрами пользователя.

Применение данной технологии позволяет практически исключить вероятность направленного подбора пароля. В частности в экспериментах злоумышленник мог осуществить подбор темпа набора за 7-10 только при возможности наблюдения набора зарегистрированного пользователя. При отсутствии такой возможности злоумышленник не смог подобрать темп набора.

Предложенный метод демонстрирует успешное применение аутентификации по клавиатурному почерку для управления доступом к информации на мобильных телефонах. Разработанное в ходе экспериментов программное обеспечение после доработки (усиления средств работы с персональной информацией пользователя, улучшения графического интерфейса, оптимизации скорости работы) может быть использовано на практике. Однако существует ряд проблем, которые требуют дальнейшего исследования.

1. Снижение вероятности FAR и FRR. Для решения данной задачи мы планируем применение более совершенных решающих механизмов. В частности, мы планируем эксперименты с быстрыми нейронными сетями и скрытыми марковскими моделями.

2. Криптографическая защита данных. В настоящее время метод обеспечивает принятие решения и управление доступом. Сами данные при этом не шифруются и могут быть извлечены. Мы планируем разработку метода генерации криптографического ключа по клавиатурному паролю подобно /5/.

Список литературы

1. *Grand J.* Introduction to mobile device insecurity, Black Hat Europe 2004 Briefing, may 2004. URL: http://www.blackhat.com/presentations/bh-europe-04/bh-eu-04-grand-mobil.pdf

2. *NetSec.* Mobile computing security threats, 2004. URL: http://www1.netsec.net/content/securitybrief/archive/2004-0_MobileSecurityThreats.pdf.

3. *Clarke N., Dowland P., Furnell S., Reynolds P., Rodwell P.* Non-Intrusive Biometric Authentication for Mobile Devices, Department of Communication and Electronic Engineering, University of Plymouth, UK, URL:

http://ted.see.plym.ac.uk/nrg/presentations/Biometrics_2002.pdf.