УДК 004.942

ЖЕСТОВАЯ АУТЕНТИФИКАЦИЯ ПРИ ПОМОЩИ ДВУХ НЕЗАВИСИМЫХ МОБИЛЬНЫХ УСТРОЙСТВ

Козлов Ю.Е.,
студент, Финансовый университет, Москва, Россия
kozlovye@yandex.ru

Аннотация. *В рамках статьи рассмотрен способ жестовой мультимодальной аутентификации в мобильных приложениях. Приведено ее место в общей классификации биометрических способов аутентификации. Рассматривается совокупность биометрических (анатомических) особенностей, позволяющих считать жестовую аутентификацию достаточно надежной. Приводится алгоритм работы жестовой аутентификации, выполняемой одновременно мобильным и запястным устройствами.*

Ключевые слова: *аутентификация; мобильное устройство; акселерометр; алгоритм.*

HARD AUTHENTICATION WITH THE TWO INDEPENDENT MOBILE DEVICES

Kozlov Yu.E.,
student, Financial University, Moscow, Russia
kozlovye@yandex.ru

Annotation. *Within the framework of the article, the method of gesture multimodal authentication in mobile applications is considered. Its place in the general classification of biometric authentication methods is given. A set of biometric (anatomical) features is considered, which makes it possible to consider gestural authentication quite reliable. An algorithm for the work of gesture authentication, performed simultaneously by a mobile and a wrist device, is given.*

Keywords: *authentication; mobile device; accelerometer; algorithm.*

С появлением новых видов небанковского обслуживания, связанных с предоставлением таких сервисов, как web-money, PayPal, Second-life, которые не имеют прямого отношения к банкам, но, тем не менее, пересекаются с историческими банковскими видами деятельности — платежами, депозитами, кредитами и т.д. Структура банковского мобильного сервиса должна двигаться в направлении развития этих технологий, в ключевых продуктах, процессах, компетенциях. Очевиден тренд на снижение барьеров и выход банков за границы традиционной банковской деятельности.

Банковская индустрия наряду с телекоммуникационной наиболее глобализированная. Как нет границ у Интернета, так нет их и у капитала. Свободное перетекание средств из индустрии в индустрию, из страны в страну заставляет участников рынка сегодня уделять особое внимание развитию технологий, которые, вполне возможно,

Научный руководитель: ***Дворянкин С.В.,*** *доктор наук, профессор кафедры информационной безопасности, Финансовый университет.*

Рис. 1. **Пример жеста, который может служить для аутентификации**

не были бы нужны, если бы не эра глобализации. Но глобализация рынка капиталов, требующая молниеносных решений, заставляет банки двигаться вперед и внедрять инновации [1].

Одним из важных направлений такого развития является внедрения новых банковских сервисов, использующих мобильное устройство в качестве средства проведения банковских операций. Основной задачей для таких сервисов является обеспечение безопасности, что в первую очередь связано с процедурами надежной аутентификации. Усовершенствование существующих методов аутентификации и разработка новых позволяет удерживать безопасность совершаемых банковских операций с использование мобильных устройств на должном уровне.

Современные методы аутентификации клиента банка можно подразделить на три категории:

1) то, что пользователь знает. Этот метод основан на секретной информации, которую человек знает и применяет в целях аутентификации: пароль, ключевая фраза или персональный идентификационный номер (PIN);

2) то, чем пользователь обладает. Удостоверение личности, паспорт, банковская карта, USB-токен, различные ключи в других форматах — все это является примером того, чем пользователь владеет и может использовать для своей идентификации;

3) то, что есть сам пользователь. Этот метод основан на физической или поведенческой особенности, которая является уникальной для человека и помогает его идентифицировать. Известными биометрическими методами аутентификации являются отпечатки пальцев, голос, сканирование радужной оболочки глаза, сканирование ладоней или геометрия руки, динамическая подпись.

Мало кто сегодня сомневается в том, что в будущем будет осуществлен переход на третью группу методов аутентификации клиента в банковской сфере, и для этого есть весомые аргументы. Эффективность пароля зависит от секретности, которая может быть раскрыта посредством сниффинга, троянского коня, подслушивания и слежения, социальной инженерии и т.д. Группа «то, что пользователь знает» относительно проста для проникновения. Чаще всего пользователи, чтобы не забыть или не ошибиться с паролем, записывают его на вещественные или электронные носители, что делает его уязвимым для кражи [2].

Методика мультимодальной жестовой аутентификации, использующая в качестве биометрического материала специальный жест человека, является одним из направлений развития биометрических методов аутентификации в мобильных приложениях, способных повысить защищенность денежных средств от краж с использованием уязвимостей в аутентификации удаленного банковского обслуживания.

Несмотря на то что биометрическая аутентификация не является решением всех проблем, этот метод избавляет от ввода паролей и, следовательно, более прост и доступен рядовому пользователю.

Суть методики заключается в выполнении специального заранее придуманного аутентифицирующего жеста мобильным устройством. С целью увеличения надежности при воспроизведении жеста его регистрация производится

Рис. 2. **Классификация биометрических методов**

двумя устройствами одновременно — мобильным устройством и запястным устройством.

На *рис. 1* представлен пример жеста, который может служить для аутентификации. Жирной точкой на рисунке обозначается начало траектории, а стрелкой указывается ее направление.

В качестве запястного устройства может служить устройство, имеющее акселерометр, например умные часы или фитнес-браслет. Ассортимент данных устройств в настоящее время достаточно широк, а цена самых бюджетных моделей около 800 руб.

Методика жестовой аутентификации подразумевает определение характеристик устройства в пространстве — эту задачу позволяет решить встроенный акселерометр. В настоящее время акселерометром оснащаются практически все мобильные устройства — смартфоны, планшеты, умные часы, фитнесс-браслеты и т.п. Основным назначением этого датчика является предоставление информации о текущем ускорении устройства, точнее, разности ускорения устройства и ускорения свободного падения. В состоянии покоя показания датчика совпадают с вектором ускорения свободного падения.

Использование запястного устройства совместно с мобильным имеет ряд преимуществ и позволяет увеличить надежность аутентификации. Оба устройства плотно взаимодействуют друг с другом и персонифицированы, например запястное устройство может служить, при необходимости, ключом к разблокировке смартфона. Такая функция уже внедрена во многие фитнес-браслеты и широко используется.

К недостаткам способа следует отнести необходимость наличия двух устройств, а также необходимость перекалибровки жеста в случае замены любого из устройств. Данный способ аутентификации будет особенно интересен людям, привыкшим к ношению фитнес-браслетов или умных часов.

Работы по использованию жеста устройством для аутентификации начали появляться с 2009 г., однако по некоторым причинам они не получили

Рис. 3. **Алгоритм работы аутентификации, использующей мобильное и запястное устройство одновременно**

широкого распространения. В настоящее время результаты данных работ представлены алгоритмом uWave, использующим в качестве основы методику динамической трансформации шкалы времени — DTW (Dynamic Time Warping) [3]. Как показали эксперименты, надежность методики, использующей только одно устройство, не очень высока, вероятность ошибок первого ли второго рода равна 1,4%. Кроме того, вероятность подделки аутентифицирующего жеста составит 10%, если злоумышленник видит, как пользователь выполняет свой жест [4].

Мультимодальная аутентификация при помощи двух независимых устройств относится к биометрическим методам. На *рис. 2* представлена классификация биометрических методов по принципу действия и способу использования.

Аутентификацию при помощи жеста мобильным и одновременно запястным устройствами, согласно предложенной классификации, можно отнести к динамическому мультимодальному способу. Здесь, кроме воспроизведения известного только пользователю жеста, в аутентификации будут участвовать и биометрические (анатомические) особенности конкретного человека. Об этих особенностях будет сказано ниже.

Длительность жеста, предположительно, составляет несколько секунд, а значит, вычисления, необходимые для принятия решения, может проделать мобильный телефон, так как объем данных, при скорости акселерометра примерно 200 отсчетов в секунду, будет не более 500 Кб. Следовательно, способ использования данного метода может быть любой — и для доступа к локальным ресурсам, и для доступа к удаленным.

Представленный способ аутентификации может называться мультимодальным в силу того, что аутентификация, кроме известного только пользователю жеста, одновременно использует несколько биометрических характеристик. В частности, аутентифицирующий жест несет в себе особенности жестикуляции, присущие только конкретному человеку. Одновременно,

при использовании запястного устройства, в жесте участвуют некоторые особенности строения руки человека.

Как известно, рука человека представляет три шарнирно соединенных звена: плечо, предплечье и кисть. Нетрудно подсчитать, что плечо имеет пять степеней подвижности. Рука, оставаясь прямой, может поворачиваться вокруг всех трех осей (три степени подвижности), а само плечо может двигаться взад-вперед и вверх-вниз (еще две степени подвижности). Предплечье, соединенное с плечом в локтевом суставе, имеет две степени подвижности: сгиб руки в локте и вращение предплечья вокруг локтевого сустава. Кисть руки имеет еще две степени подвижности: она может двигаться относительно предплечья в двух плоскостях.

Рука человека (не считая подвижности пальцев) имеет девять (5 + 2 + 2) степеней подвижности.

Предполагается, что при выполнении аутентифицирующего жеста человек держит мобильное устройство, зажав его между большим пальцем и кистью, как показано на *рис. 1*. В этом случае можно считать, что мобильное устройство относительно кисти неподвижно. Тогда кроме уникальности самого жеста, при снятии показаний акселерометра с запястья на траекторию движения будут оказывать влияние следующие анатомические особенности конкретного человека:

- кисть относительно предплечья имеет две степени свободы, которые используются людьми в соответствии с их индивидуальными особенностями;
- размер предплечья и кисти будет влиять на расстояние между мобильным и запястным устройством, а значит, соотношение фигур, описываемых мобильным и запястным устройством, для людей с разной длинной руки будет отличаться;
- естественное положение локтя человека, которое будет определять положение предплечья относительно плечевого сустава в горизонтальной плоскости, будет влиять на разницу траекторий фигур мобильного и запястного устройства. Например, для более полных людей локоть будет смещен по горизонтали.

На *рис. 3* представлен алгоритм работы аутентификации, использующей мобильное и запястное устройство одновременно.

Расстояния D_1, D_2, D_3, получаемые в результате работы алгоритма DTW или FastDTW, являются расстояниями Левинштейна, которые находятся следующим образом: пусть строки S_1 и S_2 две строки над некоторым алфавитом длиной M и N соответственно. Расстояние Левенштейна для каждого из $d(S_1, S_2)$ рассчитывается по рекуррентной формуле:

$$d(S_1, S_2) = D(M, N),$$

где $D(M, N)$:

$$D(i,j) = \begin{cases} 0; & i=0, j=0 \\ i; & j=0, i>0 \\ j; & i=0, j>0 \\ \min\begin{pmatrix} D(i,j-1)+1, \\ D(i-1,j), \\ D(i-1,j-1)+m(S_1[i], S_2[j]) \end{pmatrix}; & j>0,\ i>0, \end{cases}$$

где $m(S_1[i], S_2[j])$ равна нулю, если $S_1[i] = S_2[j]$, и единице в противном случае. Очевидно, что $d(S_1, S_2) = 0$, если $S_1 = S_2$.

Список источников

1. *Орловский В.М.* Офисы будущего // Прямые инвестиции. 2014. № 9. С. 76–79.
2. *Шакер И.Е.* Использование биометрической аутентификации и перспективы ее применения в банковской системе России // Экономика. Налоги. Право. 2016. Вып. № 5. С. 85–86.
3. *Jiayang L., Zhen W., Lin Z., Jehan W., Venu V.* uWave: Accelerometer-based Personalized Gesture Recognition and its Applications. 2009. URL: http://www.ruf.rice.edu/ ~mobile/publications/liu09percom.pdf (дата обращения: 05.05.2016).
4. *Jiayang L., Lin Z., Jehan W., Venu V.* User Evaluation of Lightweight User Authentication with a Single Tri-Axis Accelerometer. 2009. URL: http://www.ruf.rice.edu/ ~mobile/publications/liu09mobilehci.pdf (дата обращения: 05.05.2016).