Д. А. Соколов

ИСПОЛЬЗОВАНИЕ КЛАВИАТУРНОГО ПОЧЕРКА ДЛЯ АУТЕНТИФИКАЦИИ В РАСПРЕДЕЛЕННЫХ СИСТЕМАХ С МОБИЛЬНЫМИ КЛИЕНТАМИ

В настоящее время бизнес все больше уходит в электронную среду, где проще вести дела и проще поддерживать контакты с партнерами. Однако в то же время это упрощает и задачу преступников по получению конфиденциальной информации, представляющей коммерческую тайну или персональные данные сотрудников. По мере того как повышается информационная культура общества, люди начинают понимать, что их личные данные тоже относятся к тому, что имеет смысл защищать.

Стоит заметить, что мобильные технологии и удаленный доступ по беспроводным сетям стали очень популярны. В настоящее время основные усилия в сфере обеспечения безопасности мобильных сетей направлены на защиту самих коммуникаций, т. е. шифрование радиосигналов, и аутентификацию оборудования в сети за счет использования IMEI и SIM. В то же время недостаточно внимания уделяется обеспечению легитимности самого пользователя мобильного устройства, так как в большинстве случаев аутентификация ограничивается вводом простого PIN-кода. Когда традиционные методы аутентификации были просто перенесены в мобильную среду, разработчики не учитывали ее особенностей, а потому они получились далеко не идеальными. Таким образом, необходимо искать альтернативные методы аутентификации, которые отвечали бы всем требованиям, связанным с особенностями мобильных устройств.

В данной работе рассматривается возможность использования различных биометрических методов аутентификации для мобильных устройств. В статье представлена информация о разработанной автором системе аутентификации и о результатах ее тестирования.

Применимость биометрических методов к мобильным устройствам

Применимость различных биометрических методов в мобильных устройствах во многом зависит от имеющегося в наличии аппаратного обеспечения. Из-за цены, а также из-за понижающейся мобильности, пользователи вряд ли захотят покупать дополнительное оборудование, если только оно не принесет также и практическую пользу, например в случае с камерой, которую можно использовать не только для распознавания лица, но и для обычных фотографий. Однако в общем случае можно сказать, что для мобильных устройств применимы лишь те биометрические методы, которые не требуют дополнительного оборудования и могут быть реализованы на существующих устройствах. Примерный перечень подходящих методов приведен в таблице 1.

Таблица 1. Биометрия, применимая в мобильных устройствах.

Мобильный телефон	КПК	Ноутбук
• Распознавание голоса • Клавиатурный почерк • Распознавание лица • Распознавание радужной оболочки глаза	• Распознавание голоса • Распознавание лица • Распознавание радужной оболочки глаза • Распознавание подписи	• Клавиатурный почерк • Сканирование отпечатка пальца • Распознавание лица • Распознавание радужной оболочки глаза

В данной работе рассматриваются только мобильные телефоны, так как их функциональность быстро растет, приближаясь к функциональности карманных компьютеров, а именно: появляются возможности ведения электронной коммерции, растет объем памяти, вследствие чего на телефонах

может оказываться конфиденциальная информация. Из тех четырех подходов, что приведены в таблице, последние два связаны с серьезными проблемами, так как встроенные камеры хоть и присутствуют почти во всех современных телефонах, часто неспособны справиться со сложными условиями съемки, такими как меняющиеся условия освещения, позиция съемки и т. п. Распознавание голоса заслуживает большего внимания, так как существующие алгоритмы дают удовлетворительные результаты, но окружающая обстановка оказывает слишком сильное влияние и аутентификация в шумном месте станет практически невозможной. В то же время использование клавиатурного почерка позволяет организовать аутентификацию в разной форме, т. е. сделать ее непрерывной и прозрачной для пользователя или однократной. Кроме того, в таком случае исчезает фактор негативного отношения пользователей к биометрическим системам, так как по форме процесс аутентификации будет неотличим от простого ввода пароля. На основании проведенного анализа в качестве биометрического аутентификационного фактора был выбран клавиатурный почерк. Более подробно принципы анализа клавиатурного почерка описаны в работах [1, 2, 3].

Система многофакторной аутентификации

В качестве платформы для разработки приложения была выбрана технология J2ME, так как она поддерживается подавляющим большинством мобильных телефонов и таким образом позволит покрыть значительную часть рынка мобильных устройств. Разработанная система может как функционировать автономно, так и быть интегрированной в более крупное решение, например, как часть системы веб-аутентификации. Принцип работы системы в целом можно описать по шагам следующим образом:

• клиент получает при регистрации в системе, например в системе мобильного банкинга, приложение для своего мобильного телефона и индивидуальный вектор инициализации, который будет уже зашит в это приложение. Таким образом, все клиенты могут иметь одинаковую программу, а вектор инициализации будет у каждого свой;

• при аутентификации в системе пользователь вводит свой пароль в систему, правильность ввода этого пароля проверяется по его клавиатурному почерку и в результате выносится решение об авторизации пользователя;

• в случае успешно пройденной аутентификации на основе вектора инициализации и текущего времени генерируется одноразовый пароль, который пользователь может применять для аутентификации в основную систему.

Настоящая реализация системы анализа клавиатурного почерка использует две характеристики: длительность нажатия кнопок и временные интервалы между их нажатиями. Для удобства в дальнейшем и те, и другие будут называться временными засечками, так как между ними нет принципиальной разницы. В ходе регистрации пользователя в системе вычисляется среднее значение для каждой из его временных засечек. Пусть $m_j(v_i)$ — среднее значение величины v_i после j-й итерации ввода пароля при регистрации, i — порядковый номер временной засечки в векторе, v_{ij} — значение i-й временной засечки при j-м вводе пароля. Тогда среднее значение временных засечек на каждом шаге определяется следующим выражением:

$$m_j(v_j) = \frac{(j-1)m_j - 1(v_i) + v_{ij}}{j} \quad . \tag{1}$$

Для каждого среднего таким же образом вычисляется также и среднее отклонение $\sigma_j(v_i)$:

$$\sigma_j(v_i) = \sqrt{\frac{(j-2)\sigma^2_{j-1}(v_i) + (v_{ij} - m_j(v_j))^2}{j-1}} \quad . \tag{2}$$

Был проведен предварительный анализ для выбора методов сравнения образцов. Существуют два класса таких методов — статистические и основанные на нейронных сетях. Несмотря на то что вторые дают лучшие результаты, их использование на мобильных устройствах нецелесообразно,

так как они требуют вычислительных возможностей, которыми телефоны не обладают. В связи с этим выбор был сделан в пользу статистических методов, а именно меры Хэмминга и гауссовой плотности вероятностей, так как первый метод — это один из самых известных методов сравнения двоичных векторов, неоднократно доказавший свою эффективность, а второй был введен в качестве эксперимента, так как до этого для анализа клавиатурного почерка не применялся только в работе [4] и оказался полезен в сочетании с другим статистическим методом. Мера Хэмминга вычисляется следующим образом. Для каждой временной засечки вычисляются две дополнительные величины: $[min(v_i), max(v_i)]$, которые определяют диапазон, характерный для пользователя. В процессе аутентификации для каждого параметра проверяется, попадает ли он в заданный диапазон. Чем больше значений выпадает, тем больше оценка. Для данной конкретной реализации необходимо уточнить, что границы диапазонов для каждой временной засечки вычислялись следующим образом:

$$\min(v_i) = m(v_i) - t[L, (1 - P_i)] * \sigma(v_i); \quad (3)$$

$$\max(v_i) = m(v_i) + t[L, (1 - P_i)] * \sigma(v_i), \quad (4)$$

где L — количество образцов, полученных на этапе регистрации пользователя, P_i — требуемая величина коэффициента FRR, а $t[L, (1 - P_i)]$ — коэффициент Стьюдента, соответствующий этому значению FRR.

Пусть k — длина вектора временных засечек, $i \in [1, k]$, v_i — значение i-й временной засечки во введенном векторе, $m(v_i)$ — среднее значение данного элемента вектора, полученное при регистрации, $\sigma(v_i)$ — среднее отклонение этого значения, также хранимое с этапа регистрации, тогда оценка S, даваемая алгоритмом гауссовой плотности вероятностей для сравниваемых векторов, определяется следующим выражением:

$$S = \frac{\sum_{i=1}^{k} S_i}{k}, \quad (5)$$

где

$$S_i = e^{\frac{(v_i - m(v_i))^2}{2\sigma^2(v_i)}}. \quad (6)$$

Для генерации одноразового пароля была использована реализация однонаправленной функции по алгоритму SHA-1, так как данная подсистема создавалась в соответствии со стандартом [5], а среди однонаправленных функций, предложенных там, SHA-1 является наиболее стойкой. На вход алгоритму SHA-1 подается строка, состоящая из секретного вектора инициализации, полученного клиентом вместе с приложением, и текущего времени, с округлением до минуты. Таким образом, срок действия каждого одноразового пароля — 1 минута. Результат работы алгоритма, составляющий 160 бит, приводится к 64 битам, как это предлагается в стандарте [5]. Однако и 64 бита в шестнадцатеричной форме представляют собой не самый удобный для ручного ввода набор данных, поэтому, руководствуясь теми же указаниями, было решено приводить одноразовый пароль к более удобному для ручного ввода виду, а именно к 6 словам длины 4 или менее символа, выбираемым их словаря, содержащего 2048 таких слов. Полученные 64 бита представляются в двоичном виде, в конце добавляются два бита контрольной суммы, эти 66 бит разбиваются на 6 групп по 11, и каждой группе ставится в соответствие слово, индекс которого в словаре совпадает с ней по значению.

Тестирование системы

Для анализа точности работы полученной системы было проведено двухэтапное тестирование. Первый этап выявил неэффективность алгоритмов в их изначальном виде, и по результатам этого тестирования был составлен и реализован список мер, предположительно повышающих точность системы, а именно: проверить работу двух реализованных алгоритмов в отдельности, проверить работу системы при паролях разной длины: 7, 10, 11 цифр, тогда как в первом тестировании использовался

пароль фиксированной длины — 11 цифр, а также увеличить количество итераций ввода пароля при регистрации пользователя в системе с исключением наихудшего из полученных образцов.

Реализация вышеприведенных мер позволила определить, что использование гауссовой плотности вероятностей для анализа клавиатурного почерка неэффективно и ведет к снижению общей точности работы системы. Кроме того, был сделан вывод о том, что увеличение длины пароля необязательно ведет к снижению коэффициентов ложного доступа и ложного отказа в доступе, так как лучшие показатели были достигнуты при длине пароля в 11 символов, но 10-значные пароли уступили 7-значным. Это может объясняться тем, что использование более длинного пароля хоть и дает большее число временных засечек, но ведет к менее стабильному его вводу.

Основными характеристиками биометрических систем аутентификации являются коэффициенты ложного доступа и ложного отказа в доступе, поэтому целью данного тестирования было именно получение оценок для этих коэффициентов. Итоговые параметры системы составили 0,04 для коэффициента ложного доступа и 0,09 для коэффициента ложного отказа в доступе, они были достигнуты при использовании паролей длиной в 11 цифр и анализе сходства образцов по мере Хэмминга с пороговой величиной 0,65. Готовых реализаций подобных систем пока не существует, поэтому сравнивать полученные результаты можно только с другими исследованиями в этой области. В [6] приведен обобщенный список таких работ с их результатами, откуда можно сделать вывод, что параметры разработанной системы не уступают лучшим из аналогичных работ.

Полученные значения ошибок приводят к выводу, что использование клавиатурного почерка в качестве единственного фактора аутентификации на мобильном устройстве пока не позволяет достичь достаточной точности, однако не стоит забывать, что разработанная система реализует двухфакторную аутентификацию, так как вводимый пароль остается секретной информацией, которой должен обладать пользователь. Таким образом, применение биометрии, в частности клавиатурного почерка, в сочетании с используемым в настоящее время подходом только повысит общую надежность системы аутентификации. Кроме того, можно рассмотреть возможность использования различных профилей доступа, т. е. разграничение доступа к информации разного уровня конфиденциальности в зависимости от предоставленных аутентификационных факторов.

Заключение

В данной работе рассматривалась возможность применения биометрических методов аутентификации к мобильным устройствам. Был сделан вывод о том, что клавиатурный почерк наилучшим образом подходит в качестве аутентификационного фактора для мобильных телефонов. Была реализована система аутентификации в виде приложения на платформе J2ME, позволяющая регистрировать пользователей в системе, проводить их последующую аутентификацию и генерировать для легальных пользователей одноразовый пароль для дальнейшего использования. Было проведено тестирование системы с оценкой полученных параметров и сделан вывод о ее практической применимости.

СПИСОК ЛИТЕРАТУРЫ:

1. *Olzak T.* Keystroke Dynamics: Low Impact Biometric Verification. 2006.
2. *Ilonen J.* Keystroke dynamics. 2008.
3. *Monrose F., Rubin A.* Keystroke Dynamics as a Biometric for Authentication. 1999.
4. *Teh P. S., Teoh A., Ong T. S., Neo H. F.* Statistical Fusion Approach on Keystroke Dynamics // Proceedings of the Third International IEEE Conference on Signal-Image Technologies and Internet-Based System, Shanghai. 2007. P. 918–923.
5. RFC 2289 A One-Time Password System.
6. *Buchoux A., Clarke N. L.* Deployment of Keystroke Analysis on a Smartphone. 2008.