УДК 004.056.53

АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ ПО КЛАВИАТУРНОМУ ПОЧЕРКУ

Е.В. Сухаревская

студент кафедры информационной безопасности

Волгоградский государственный университет

Аннотация: Обеспечение информационной безопасности любой информационной системы – одна из главных задач мира IT- технологий. В основе этой защиты лежит самая распространенная основная угроза – несанкционированный доступ к системе. Предотвратить попытку несанкционированного доступа можно, обеспечив процедуры разграничения доступа в систему. Такими процедурами являются идентификация и аутентификация. В данной статье были рассмотрены основные характеристики, достоинства и недостатки биометрических систем аутентификации, их применение в современном мире, их актуальность и причины роста распространения в мире. Для более подробного рассмотрения был выбран алгоритм биометрической аутентификации, основанный на клавиатурном почерке. Также в статье был описан принцип его работы, достоинства и недостатки, применение данного алгоритма и преимущество в сравнении с другими биометрическими системами аутентификации. Далее был описан алгоритм его работы, который разделяется на три этапа. Первый этап заключается в регистрации пользователя и создании базы эталонных значений параметров, то есть допустимых значений в виде интервалов. Второй этап предусматривает тестирование системы на попадание параметров в заданные эталонные интервалы, и на их основе формирование порогового значения для возможных допущений ошибок. И наконец, третий этап – это проведение аутентификации пользователя и сравнение полученного значения меры Хэмминга с пороговым значением с последующим принятием решения о допуске или не допуске пользователя в систему.

Ключевые слова: аутентификация, система аутентификации, информационная система, защита информации, биометрическая аутентификация, биометрия, клавиатурный почерк.

USER AUTHENTICATION BY KEYBOARD HANDWRITING

E.V. Sukharevskaya

Student of Information Security Department

Volgograd State University

Annotation: Information security of any information system is one of the main tasks of the world of IT - technologies. The main of this protection is the most common and the main threat – unauthorized access to the system. It is possible to prevent attempt of unauthorized access by having provided identification and authentication. In this article were discussed the main characteristics, advantages and disadvantages of biometric authentication systems. For a more detailed analysis there was chosen the algorithm of biometric authentication based on keyboard handwriting. The article also describes the principle of its operation, advantages and disadvantages, the use of this algorithm. Then there was described the algorithm of its work, which is divided into three stages. The first step is to register the user and create a database of reference parameter values. The second stage involves testing the system to get the parameters in the specified reference intervals, and on their basis the formation of a threshold for possible error assumptions. Finally, the third stage is to conduct user authentication, and the comparison of the measure values of the Hamming with a threshold value for subsequent decision on admission or non-admission of the user into the system.

Keywords: authentication, authentication system, information system, protection of information, biometric authentication, biometric, keyboard handwriting.

В современном мире любая информационная система имеет слабые места и может быть подвержена атакам. По статистике наиболее распространенной угрозой для информационной системы является попытка несанкционированного доступа к данным. Обеспечение информационной безопасности информационной системы означает внедрение комплексной системы защиты доступа к информации для предотвращения попыток несанкционированного доступа (НСД) к данным.

Основными процессами в любой системе защиты доступа от НСД являются идентификация и аутентификация [1, С. 238]. Все большую популярность в мире обретают биометрические системы аутентификации, удостоверяющие личность пользователя по его биометрическим данным [2, С. 135]. Не так давно такие системы применялись в системах для особо охраняемых зоны, но сейчас стоимость установки такой системы постепенно снижается и распространение по миру увеличивается.

Биометрические системы аутентификации обладают рядом преимуществ. К примеру, они признаны самыми комфортными и удобными для пользователей, так как для аутентификации им не нужно ничего запоминать или носить с собой [3, С. 127]. Считывающие устройства систем биометрической аутентификации не допускают ошибок, в отличие от пользователей, то есть пользователь никак не может ошибиться, как, к примеру, при вводе пароля. Также нельзя передать свою биометрическую характеристику другому лицу [4, С. 174]. К недостаткам биометрических систем можно отнести возможность ошибок первого и второго рода, а именно: допуск к системе лиц, не имеющих полномочий, что возможно при поднесении муляжа к сканеру отпечатка пальца, и не допуск пользователей, имеющих полномочия, к примеру, из-за простуды при аутентификации на основании распознавания голоса.

Основными характеристиками любой биометрической системы аутентификации как раз и являются ошибки первого и второго рода. Их называют FAR (False Acceptance Rate) и FRR (False Rejection Rate), или простыми словами - «ложная тревога» или «пропуск цели». FAR характеризует вероятность ложного совпадения характеристик двух разных людей, а FRR – вероятность отказа в доступе пользователю, который имеет допуск.

Все биометрические системы аутентификации основываются на биометрических характеристиках человека, которые могут быть статическими и динамическими. К системам, основанным на статических методах, а именно на физиологии человека, относятся: аутентификация по отпечатку пальца, по радужной оболочке или сетчатке глаза, по геометрии руки или лица, или по термограмме лица. К системам, основанным на динамических методах, т.е. на поведении и на особенностях, характерных для уникальных

подсознательных движений, относятся: аутентификация по голосу, по рукописному или клавиатурному почерку.

В данной статье мы рассмотрим алгоритм биометрической аутентификации по клавиатурному почерку, поэтому рассмотрим этот метод более подробно. Клавиатурный почерк пользователя – это поведенческие характеристики человека. Такой метод аутентификации обладает необходимой стабильностью для проведения аутентификации без использования дополнительного оборудования, так как с помощью обычной клавиатуры и специализированного программного обеспечения считываются исходные данные пользователя. В качестве исходных данных принимаются интервалы времени между нажатием каждой клавиши на клавиатуре, время удержания каждой клавиши, то есть считывается динамика работы с клавиатурой. Интервал времени между нажатием клавиши характеризуют непосредственно темп работы пользователя с клавиатурой, а время удержания клавиши – стиль работы, то есть резкими ударами или плавными нажатиями осуществляется ввод.

Аутентификация по клавиатурному почерку все больше находит применение в современном мире из-за своей простоты внедрения и реализации. К тому же такая система является дешевой в сравнении с её другими аналогами биометрических систем аутентификации. Особенно удобна такая система для пользователя, потому что от него не требуется никаких действий, кроме ввода контрольной фразы или пароля.

К сожалению, такая система обладает и недостатками. Во-первых, может возникнуть нестабильность характеристик, которая может быть вызвана улучшением навыков работы с клавиатурой, или наоборот из-за старения организма. Вследствие этого такой системе необходимы постоянные корректировки и обновления баз эталонов пользователей. На характер работы с клавиатурой влияют и временные факторы, к примеру, утром и вечером динамика работы будет разной, что говорит о вероятности возникновения ошибок аутентификации. Поэтому такие ошибки должны быть нейтрализованы с помощью постоянных изменений характеристик после каждой успешной аутентификации пользователя, то есть с помощью корректировок баз эталонных моделей пользователя. Применение таких систем осуществляется в основном в тех организациях, где осуществляется клавиатурный ввод информации.

Аутентификация по клавиатурному почерку, в силу невозможности отделения биометрических характеристик от человека, обеспечивают высокую в сравнении с другими методами аутентификации точность, удобство применения для пользователя и невозможность отказа от факта авторства.

На сегодняшний день существует три алгоритма биометрической аутентификации по клавиатурному почерку:

1) Алгоритм, анализирующий клавиатурный почерк во время ввода пароля;
2) Алгоритм, анализирующий клавиатурный почерк после ввода дополнительного текстового фрагмента или фразы;
3) Алгоритм, который постоянно производит скрытый мониторинг клавиатурного почерка пользователя;

Первый алгоритм обладает наиболее высоким быстродействием в сравнении с другими алгоритмами, так как для получения биометрических данных пользователю необходимо ввести только пароль. Но дать большие гарантии в точности аутентификации нельзя из-за того факта, что пароли бывают слишком короткие. Также будет невозможно обнаружить подмену в случае, если пользователь прошел аутентификацию в системе и оставил рабочее место без присмотра, в то время как злоумышленник занял его место для корыстных целей. Обычно пароль пользователя может состоять от 10-30 символов. Из-за такого небольшого количества требуется дополнительно настраивать порог доступа, чтобы снизить ошибки первого и второго рода.

Второй алгоритм, который анализирует клавиатурный почерк после ввода дополнительного текстового фрагмента или фразы, в свою очередь, имеет преимущество перед первым алгоритмом в виде высокой точности аутентификации. Но характеристику «быстродействие» нельзя отнести к данному алгоритму, потому что для ввода дополнительной фразы или текстового фрагмента, длина которых часто превышает 1000 символов, требуется достаточно много времени. Также эта процедура может вызвать у пользователя негатив из-за возможно частого прохождения процедуры аутентификации с вводом длинного фрагмента текста.

Для работы данного алгоритма необходимо применение вероятностно-статистического метода, то есть сбор статистики из выборки временных значений. Непосредственно элементом выборки является время удержания клавиши. Эталонное представления пользователя создается в режиме обучения. В данном режиме собираются статистические данные о нажатиях каждой клавиши. В результате формируется трехмерная таблица, состоящая из N столбцов, где N – количество нажатых клавиш (таблица 1). Также определяется конечное число нажатий определенной клавиши K, где K - количество нажатий, данные о которых необходимо создать для эталонной модели. Такое число будет отражать количество строк в таблице. В каждую ячейку таблицы будет заноситься значение о времени удержании конкретной клавиши в определенный раз нажатия.

Таблица 1 – статистический сбор данных

Кл1	**…**	**КлN**
Время 1-го удержания клавиши	…	Время 1-го удержания клавиши
…	…	…
Время K-го удержания клавиши	…	Время K-го удержания клавиши

После сбора всех данных подсчитывается математическое ожидание каждой выборки (для каждой клавиши), и эталон сохраняется в учетной записи.

Перед аутентификацией пользователь идентифицирует себя, то есть вводит пароль. После этого проходит аутентификацию. Пользователю предоставляется определенный или случайный текстовый фрагмент, длина которого обычно может составлять до 5000 символов. По ходу ввода пользователем данного ему фрагмента, программа считывает статистические данные и сравнивает их с сохраненными эталонными значениями математических ожиданий различных выборок.

Третий алгоритм, который производит скрытый мониторинг клавиатурного почерка пользователя, также обеспечивают довольно высокую точность, но в реализации работы затрачивают намного больше ресурсов. Преимуществом данного алгоритма является возможность распознать злоумышленника в том случае, если пользователь авторизовался в системе, но временно отсутствовал, а в это время злоумышленник занял его место и продолжил работу с системой. При такой ситуации программа аутентификации заблокирует систему, чтобы предотвратить хищение защищаемой информации, с возможностью разблокировки системы администратором.

В данном алгоритме постоянно рассматриваются фрагменты фраз из 10-40 символов. Такое количество символов может быть аргументировано интервалом копирования пользователя, подразумевающее собой то количество символов, которое может быть напечатано пользователем после однократного ознакомления с текстом. Данная величина может зависеть от различных характеристик человека: как от опыта его работы, так и от физиологических особенностях (память, состояние организма и т.д.). Инициализируется массив из 10-40 символов, и в него динамически заносятся характеристики в виде времени удержания клавиши. Данный массив динамически обновляется по ходу введения новых символов пользователем. Элементы, которые были введены ранее, будут удалены и время удержания клавиш рассчитывается по новым добавленным элементам.

Рассмотрим более подробно алгоритм биометрической аутентификации, который анализирует клавиатурный почерк во время ввода пароля. Данный алгоритм использует при наборе на клавиатуре парольной фразы для аутентификации пользователя следующие биометрические характеристики: время нажатия (td_i) и время отпускания (tu_i) клавиши, $i = 1, \dots, n$, где n – длина парольной фразы, и полное время набора парольной фразы T. По данным параметрам формируется вектор биометрических параметров V.

Для создания эталонной модели пользователя необходимо 30 векторов V, то есть пользователь должен 30 раз ввести парольную фразу. После анализа имеющихся 30 реализаций вектора биометрических параметров формируются интервалы допустимых значений для каждого параметра, которые записываются в системе как эталонные для каждого пользователя.

Далее происходит второй этап регистрации пользователя - тестирование системы. На данном этапе пользователь повторно вводит парольную фразу 10 раз. И теперь система проверяет параметр каждого вектора на попадание в эталонный интервал. Для данной задачи и для каждого вектора биометрических параметров создается вектор E, который состоит из нулей и единиц. Если параметр попадает в эталонный интервал, в вектор записывается 0, иначе – 1. Предположим, что существует наилучший вектор E*, который состоит из одних нулей. Такой вектор предполагает попадание каждого параметра в свой интервал. Теперь, чтобы определить, как отличать легитимного пользователя от нелегитимного, введем понятие порогового значения ошибок при аутентификации, т.е. значение, определяющее, сколько раз параметр полученного вектора не попадет в интервал эталонных значений. Для определения порогового значения необходимо ввести расстояние Хэмминга P между наилучшим вектором и вектором тестового вектора биометрических параметров. Таких расстояний в итоге будет 10. Далее, используя полученные 10 расстояний Хэмминга, находим математическое ожидание значения меры Хэмминга P, которое и будет являться пороговым значением, то есть данное число будет отражать допустимое число несовпадений с биометрическим эталоном, то есть с характерными интервалами возможных значений параметров.

При аутентификации пользователь вводит парольную фразу, то есть предоставляет системе вектор биометрических параметров. По этому вектору также формируется вектор E и находится его расстояние Хэмминга от наилучшего вектора E*. Чтобы определить, легитимный это пользователь или нет, система проверяет полученное значение с пороговым, которое хранится в системе. Процесс принятия решения можно отобразить в следующей системе:

$$\begin{cases} E_{\text{д}} \le E_{\text{п}}, & \text{пользователь} - \text{"свой"}; \\ \text{иначе}, & \text{пользователь} - \text{"чужой"}; \end{cases}$$

Таким образом, была разработана математическая модель алгоритма биометрической аутентификации и описан процесс регистрации пользователя и его последующей аутентификации в системе. Разработанный алгоритм биометрической аутентификации по клавиатурному почерку может применяться в любой сфере деятельности человека.

Библиографический список

1. Ходашинский И.А., Савчук М.В., Горбунов И.В., Мещеряков Р.В. Технология усиленной аутентификации пользователей информационных процессов // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2011г. – №2-3 (24). – С. 236 – 248.
2. Сабанов А.Г. Об уровнях строгости аутентификации // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2012г. - № 2-1 (26). – С. 134 – 139.
3. Кусков Н.А. Исследование способов несанкционированного доступа к информации // Научный вестник Московского государственного технического университета гражданской авиации. – 2013г. - № 6 (192). – С. 127 – 129.
4. Островский А.А., Жариков Д.Н., Лукьянов В.С., Попов Д.С. Динамические методы биометрической аутентификации // Известия Волгоградского государственного технического университета. – 2010г. - № 8 . – Том 6. – С. 72-76.
5. Биометрическая идентификация [Электронный ресурс] Режим доступа: свободный http://www.tadviser.ru/index.php/Статья:Биометрическая_идентификация_(мировой_рынок) (дата обращения 02.02.18)