ТЕХНОЛОГИИ АВТОМАТИЗАЦИИ ПРОЕКТИРОВАНИЯ ПРОГРАММНЫХ СИСТЕМ

Д.Б. Ельчанинов, Н.С. Косило, Н.В. Белова

Разработан метод автоматизации процесса анализа технического задания на основе технологии синтаксического анализа текста. Показана связь между текстовым описанием технического задания, его синтаксическим деревом и актерами, объектами и сообщениями диаграмм последовательностей (UML sequence diagram). Адаптированы основные понятия теории генетических алгоритмов (ген; генотип; популяция; целевая функция; операторы отбора, скрещивания, мутации и редукции; критерии останова) к автоматизации построения этих диаграмм.

Ключевые слова: *программные системы, автоматизация проектирования, синтаксический анализ, генетические алгоритмы, UML.*

PROGRAM SYSTEMS DESIGN AUTOMATION TECHNOLOGIES

D.B. Elchaninov, N.S. Kosilo, N.V. Belova

The method of automation of process of the analysis of the specification on the basis of technology of parse of the text is developed. Relationship between the text description of the specification, its syntax tree and actors, objects and messages of UML sequence diagram is shown. The basic concepts of the genetic algorithms theory (a gene; genotype; population; target function; operators of selection, transposition, mutation and reduction; criteria of break) are adapted to automation of creation of these diagrams.

Keywords: *program systems, design automation, parse, genetic algorithms, UML.*

УДК 681.3

Н.А. Кошевая, Н.И. Мазниченко

Национальный юридический университет имени Ярослава Мудрого, Харьков

ПОДХОД К ПОВЫШЕНИЮ НАДЕЖНОСТИ ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ КОМПЬЮТЕРНЫХ СИСТЕМ ПО ДИНАМИКЕ НАПИСАНИЯ ПАРОЛЕЙ

Проанализированы возможности идентификации пользователя по особенностям клавиатурного почерка, которые используются в системах контроля и управления доступом к информационным компьютерным системам. Рассмотрены подходы по повышению надежности данного метода идентификации.

Ключевые слова: *клавиатурный почерк, идентификация пользователей ЭВМ.*

Введение

Постановка проблемы. Важнейшим аспектом информационной безопасности компьютерных систем и сетей самого широкого назначения является разграничение доступа к управлению системой и к её ресурсам. Отождествление пользователя ЭВМ - задача, решение которой позволяет организовать весь процесс управления правами доступа. Доступ пользователей к различным классам информации должен определяться идентификацией, т.е. процессом распознавания параметров, однозначно определяющих пользователя. Эффективность системы идентификации определяется качеством распознавания, зависящим от степени уникальности параметров пользователя. Целесообразным видится потребность в недорогих, простых, ненавязчивых системах идентификации, удобных для каждого пользователя. В связи с этим в последнее время все больше внимания уделяется методам идентификации пользователя по динамике подсознательных движений. Речь идет об отработанных двигательных навыках человека и о возможности использования их для идентификации и мониторинга работы пользователя компьютерных систем. Использование клавиатурного почерка в задачах идентификации пользователей представляется весьма удачным в связи с тем, что данный метод практически не требует дополнительных материальных и финансовых затрат и является приемлемым для большинства пользователей. К весомому преимуществу данного метода идентификации так же можно отнести возможность осуществлять контроль скрыто. Но, к сожалению, системы идентификации на основе клавиатурного почерка не обладают достаточной степенью надежности. Скорее всего, это является важнейшей причиной того, что системы идентификации на его основе не являются широко распространенными, невзирая на существенные преимущества. Поэтому исследование возможностей по повышению надежности и точности идентификации пользователей по данной биометрической характеристике представляется актуальным и перспективным.

Анализ литературы. Первая публикация о возможности идентификации пользователей ЭВМ по особенностям печатания на клавиатуре появилась в середине семидесятых годов предыдущего столетия в техническом бюллетене IBM [1], но без предоставления классификатора и эмпирических результатов оценки. В дальнейшем исследования в данном направлении за рубежом продолжили Форзен [2], Гайнес [3], которые использовали обычные статистические методы обработки характеристик клавиатурного

почерка. В последующие годы было предложено большое количество различных методов распознавания клавиатурного почерка: нейронные сети (Brown and Rogers, 1993; Obaidat and Sadoun, 1997; Cho et al,2000); нечеткая логика (Hussien et al, 1989; de Ru and Eloff, 1997; Haider et al, 2000; Mandujano and Soto, 2004; Tran et al, 2007); метод опорных векторов – SVM (Yu and Cho, 2003; Sung and Cho, 2005; Loy et al, 2007; Giot et al, 2009). Интерес к данному методу идентификации возрос с 2000 года, что отразилось в значительном увеличении публикаций в научной литературе по данной теме. Данная проблема изучалась в работах таких российских ученых и исследователей, как Иванов А.И., Рыбченко Д.Е., Абашин В.Г., Шарипов Р.Р., Диденко С.М., Шапцев В.А., Епифанцев Б.М., Гузик В.Ф., Галуєв Г.А., Десятерик М.Н. и других. В странах дальнего зарубежья результаты наблюдений клавиатурного почерка отражены в работах таких ученых как С. Блех, М. Умпресс, Р. Вильямс, Х. Сонг, Р. Винейбл, Би Перриг, С. Клиффорд. Но, к сожалению, в нашей стране данному научному направлению уделяется недостаточно внимания.

Цель статьи. Анализ систем идентификации пользователей компьютерных систем по клавиатурному почерку показывает, что существующие программные реализации данных систем характеризуются точностью, недостаточной для требований сегодняшнего дня. В связи с этим актуальным и целесообразным представляется поиск путей повышения точности и надежности систем идентификации пользователей компьютерных систем с использованием клавиатурного почерка.

Изложение основного материала

Идентификация пользователей по клавиатурному почерку/ Принципы, лежащие в основе применяемых методов идентификации личности пользователя, можно условно разделить на следующие: традиционная парольная защита, использование различных карт (токен, скреч-карт и т.д.), проверка биометрических характеристик человека (отпечатки пальцев, изображение сетчатки глаза, и т.п.) [4].

Наибольшее распространение в настоящее время получили методы идентификации пользователей, основанные на использовании паролей, которые, к сожалению, могут быть утеряны, украдены, т.е. скомпрометированы множеством способов. Поэтому идея комбинации стандартной парольной защиты с методом идентификации пользователя по клавиатурному почерку представляется очень удачной. В этом случае, даже если злоумышленник каким-либо образом получает доступ к паролю, доступ к компьютерной системе может быть запрещен благодаря идентификации по клавиатурному почерку, что проиллюстрировано на рис. 1. В данном случае структура идентификации по клавиатурному почерку следующая: если пользователь вводит некорректный пароль, ему моментально отказывается в доступе. Если же представлен корректный пароль, образец клавиатурного почерка данного пользователя сопоставляется с зарегистрированными образцами авторизованных пользователей. В зависимости от требуемой точности при сопоставлении пользователю может быть разрешен или запрещен доступ.

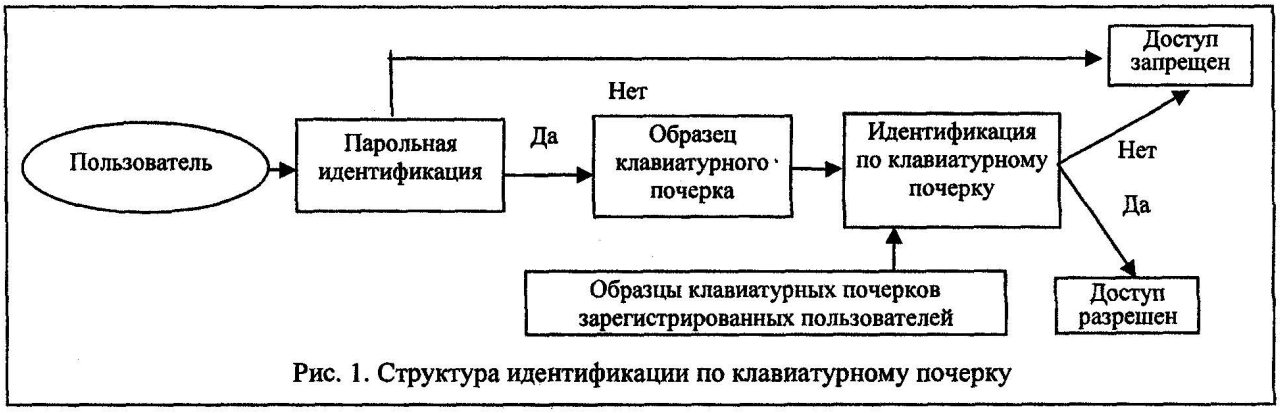

Рис. 1. Структура идентификации по клавиатурному почерку

Другие биометрические методы (технологии) также могут быть предложены для дополнения или замещения парольного метода в системах контроля доступа к информационным ресурсам компьютерных систем, например, идентификация по отпечатку пальца, по голосу, по радужной оболочке глаза и т.д. Однако перечисленные методы нуждаются в дополнительном дорогостоящем оборудовании и, что более важно, некоторые пользователи могут отказать в предоставлении своей биометрической информации. Идентификация же по клавиатурному почерку не нуждается в дополнительном оборудовании и данные о клавиатурном почерке могут быть собраны относительно легко. Каждый раз, когда пользователь набирает парольную фразу, определяется образец (шаблон) его клавиатурного почерка. Промежуток времени, когда каждая клавиша нажимается и отпускается, измеряется миллисекундами. «Нажатие» означает временной промежуток, в течение которого клавиша нажата, «интервал» – промежуток времени (скрытое состояние) между нажатием двух клавиш. В этом случае пароль из m символов может

быть преобразован в (2m+1)-мерный временной вектор. Рис. 2 иллюстрирует как строка «ABCD» может быть представлена как 9D (9-мерный) временной интервал. Отрицательное значение означает, что пользователь отпустил клавишу «D» после нажатия следующей клавиши.

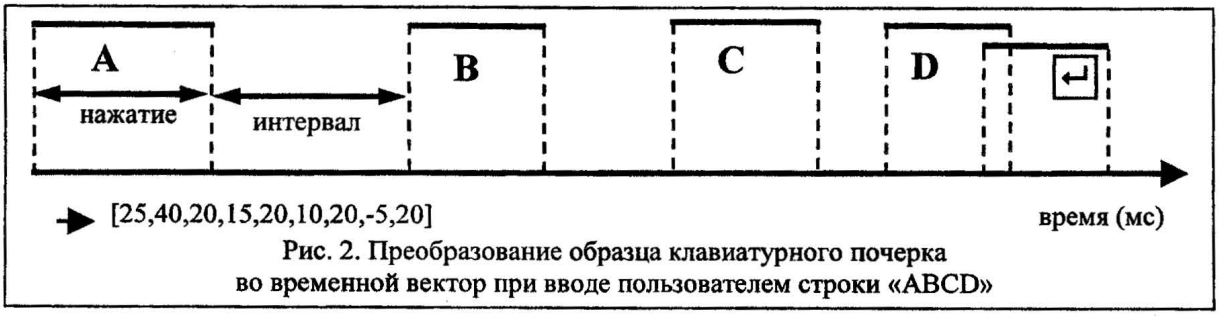

Рис. 2. Преобразование образца клавиатурного почерка во временной вектор при вводе пользователем строки «ABCD»

После того, как образцы клавиатурного почерка собраны, на их основе создается классификатор - база данных образцов (шаблонов) зарегистрированных пользователей. Затем применяются процедуры принятия решения на разрешение или отказ в доступе, которые можно систематизировать в четыре категории в зависимости от используемых алгоритмов [5]:

– статистические алгоритмы;

– вероятностно-статистические;

– на базе теории распознавания образов и нечеткой логики;

– на основе нейросетевых алгоритмов.

Применение нейросетевого подхода к данной задаче позволяет решить ряд проблем, возникающих при использовании стандартных методов статистической обработки входного потока данных. Кроме того, нейронная сеть обладает свойством фильтрации случайных помех, присутствующих во входных данных, что позволяет отказаться от алгоритмов сглаживания экспериментальных зависимостей, необходимых при статистической обработке данных [6].

Все биометрические системы идентификации пользователей, основанные на динамических характеристиках человека (анализ особенностей голоса, рукописного почерка, клавиатурного почерка) имеют схожие принципы работы и включают два режима: режим обучения и режим идентификации [7]. В режиме обучения формируется биометрический эталон личности и составляется база данных образцов зарегистрированных пользователей. В простейшем случае биометрический эталон может формироваться в виде двух векторов: вектора математических ожиданий контролируемых параметров - m(v) и вектора дисперсий этих параметров s(v).

В режиме идентификации вектор контролируемых параметров v, полученный из предъявленного образа, сравнивается решающим правилом с биометрическим эталоном. Если предъявленный вектор оказывается близок к биометрическому эталону, принимается положительное решение. При значительных отличиях предъявленного вектора и его биометрического эталона осуществляется отказ в идентификации и, следовательно, в доступе. Если протокол идентификации не слишком жесткий, то пользователю предоставляются дополнительные попытки повторной идентификации.

При анализе точности и надежности любой биометрической системы необходимы некоторые общие критерии, к которым можно отнести:

– ошибка первого рода – FRR (False Reject Rate) – вероятность того, что система «не примет» зарегистрированного пользователя;

– ошибка второго рода – FAR (False Accept Rate) – вероятность того, что система «пропустит» незарегистрированного пользователя (злоумышленника).

В некоторых системах существует возможность регуляции порога чувствительности, что позволяет гибко их настраивать в соответствии с требованиями по безопасности. Необходимо учитывать взаимосвязь этих показателей: увеличение чувствительности системы (и, как следствие, снижение достоверности ошибочного доступа - FAR) одновременно сопровождается увеличением времени идентификации и повышением достоверности ошибочного отказа - FRR. На сегодняшний день все биометрические технологии являются вероятностными, ни одна из них не способна гарантировать полное отсутствие ошибок FAR/FRR, и нередко данное обстоятельство служит основой для не очень корректной критики биометрии.

Биометрические системы также могут характеризоваться коэффициентом равной вероятности ошибок 1-го и 2-го рода (EER - Equal Error Rates), которая представляет собой точку совпадения достоверности FRR и FAR (иногда называемую Crossover Equal Error Rates). Качественная и надежная система должна иметь низкий уровень EER.

Переобучение детектора новизны с образцами злоумышленника. До недавнего времени в задачах распознавания клавиатурного почерка пользователя компьютерных систем использовались методы, основанные на так называемых ограничивающих обучающих технологиях. В данном случае при построении классификатора образцы клавиатурного почерка злоумышленника (незарегистрированного пользователя) были нежелательны и не использовались для сбора

шаблонов (образцов) клавиатурного почерка пользователей. В последнее время некоторыми авторами [8 – 12] были предложены методы обнаружения новизны, в которых детектор новизны обучается вначале только с использованием образцов зарегистрированных пользователей и позже переобучается с образцами злоумышленников, когда они становились доступными после неудачных попыток ввода пароля. В данном случае, образцы авторизованных пользователей обозначаются как нормальные, а все остальные образцы пользователей – как новые. Затем модель изучает характеристики нормальных образцов и благодаря этому в дальнейшем обнаруживает новые образцы, отличающиеся от нормальных. В геометрическом смысле детектор новизны устанавливает границы вокруг нормального образца во входном пространстве [13].

Большинство детекторов новизны имеют следующее ограничение: при обучении предполагается, что новые образцы не существуют. Так что они используют только нормальные образцы во время обучения, даже если в некоторых случаях существует небольшое количество неизвестных образцов. Допустим, была осуществлена попытка вторжения в компьютерную систему и она каким-либо образом была обнаружена. Или же авторизованный пользователь ввел свой пароль со значительными отклонениями от своего зарегистрированного образца так, что его клавиатурный почерк определен как образец злоумышленника. Хотя образцы злоумышленников не является весомыми для обучения классификатора, они могут помочь детектору новизны создать более точные и более плотные границы вокруг нормальных образцов. После того как становятся доступными образцы клавиатурного почерка злоумышленника, детектор новизны, который был обучен только с использованием образцов зарегистрированных пользователей, может быть переобучен с использованием образца злоумышленника.

Было предложено несколько методов использования новых образцов [14], [15], которые экспериментально показывают, что можно достичь большей точности при использовании образцов злоумышленника. Авторами [15] было предложено использовать новые образцы для переобучения детектора новизны, в частности, предложен так называемый метод одноклассового обучающегося векторного квантования (1-LVQ).

Расчет временного вектора образца клавиатурного почерка действительного пользователя состоит из учебных данных $U=\{(x_i; y_i)|i=1,2, \ldots ,N_U\}$, где $x_i \in R^d$ – образец клавиатурного почерка, представленный как временной вектор, а $y_i=+1$ – это его классификационная метка. Затем детектор новизны может быть обучен с этим учебным набором данных. Когда особа пытается получить доступ к системе, его образец клавиатурного почерка измеряется и вводится в детектор новизны. Если детектор признает образец как нормальный, доступ ему разрешается. Если детектор отвергает образец как новый, доступ для него будет отклонен.

Вначале доступными являются только образцы клавиатурного почерка зарегистрированных пользователей. В дальнейшем становятся доступными также образцы клавиатурного почерка злоумышленников. В этих случаях набор образцов злоумышленников может быть определен как $I=\{(x_i; y_i)\}$, $y_i=-1$. Затем может быть сформирован учебный набор данных $X=U \cup I$. Обычно количество образцов авторизованных (действительных) пользователей значительно больше, чем количество образцов злоумышленников, т.е. $|U|>>|I|$, что делает невозможным обучение классификатора сразу с двумя наборами образцов. Вместо этого детектор новизны сначала обучается с образцами зарегистрированных пользователей и позже переобучается с образцами злоумышленников, когда они становятся доступными. В данной статье среди возможных детекторов новизны, которые могут быть переобучены с образцами злоумышленников, рассматриваются SVDD и 1-LVQ.

SVDD (Support Vector Data Description – метод описания данных опорными векторами) пробует описать гиперсферу с минимальным объемом таким образом, что она окружает (охватывает) как можно больше нормальных образцов и как можно меньше новых образцов [14]. Радиус и центр гиперсферы обозначаются соответственно, как R и a. Они могут быть найдены стандартными квадратичными программными методами. В процессе идентификации неизвестный образец клавиатурного почерка z принимается как истинный пользователь, если $\|z-a\|^2 \le R^2$, или отвергается как образец злоумышленника в остальных случаях. Использование ядра Мерсера позволяет определить границы более гибкими, чем гиперсфера. Если используется радиальная базовая функция (RBF), то SVDD обеспечивает решение по существу в той же форме, что и метод Парзена или 1-SVM (одноклассовый метод опорных векторов).

Алгоритм 1-LVQ (learning vector quantization - одноклассовое обучающееся векторное квантование) является модифицированной формой оригинального LVQ [15]. Точно также как LVQ, 1-LVQ инициализируется при помощи обновления книги кодов, используя традиционный SOM (Self-organizing map – самоорганизующиеся карты Кохонена). Когда создается начальная книга кодов, используются только нормальные образцы. SOM генерирует набор кодов $W = \{w_k \mid k = 1; 2; \ldots ,K\}$, $K << N$ для представления нормальных образцов. Когда книга кодов создана, книга кодов m(x) от входного образца x и область Вороного S_k каждой книги кодов w_k определены. Когда учебный набор включает новые образцы, обучающее правило, в отличие от обычного, может быть получено следующим образом:

$$w_k \leftarrow \begin{cases} w_k, & \text{if } x_i \notin S_k, \\ w_k + \eta(x_i - w_k), & \text{if } x_i \in U_k, \\ w_k - \eta(x_i - w_k), & \text{if } x_i \in I_k, \end{cases}$$

где $U_k = U \cap S_k$ и $I_k = I \cap S_k$. Согласно этому правилу, нормальные образцы «втягивают» книги кодов, тогда как новые образцы «выталкивают» их.

Так как 1-LVQ в отличие от LVQ назначает всю книгу кодов нормальными данными, необходимо явно определить пороги. В то время как некоторые книги кодов входных образцов лежат внутри плотной областью, другие же лежат в областях, где образцы разбросаны редко. По этой причине желательно установить различные пороги для различных книг кодов. Для каждой области Вороного может быть получена гиперсфера с центром в w_k и минимальным радиусом таким образом, чтобы она окружала как можно больше нормальных образцов и небольшое количество новых образцов. Предоставленному образцу клавиатурного почерка z ставится в соответствие его код $m(z)=w_q$. Затем z принимается, если $\| z - w_q \|^2 \le (r_q^*)^2$, или отвергается в ином случае.

Экспериментальные результаты. Авторами [9] была представлена программа для измерения образца клавиатурного почерка. Данные были собраны посредством клавиатуры, соединенной с рабочими станциями 21 действительного (авторизованного) пользователя, чьи пароли представлены в первом столбце табл. 1. Многие из них не читаемы, т.к. набраны на других языках, например, «rhkdwo», «dhfpql.» – на корейском. Они просто представлены в соответствующих английских буквах относительно их положения на клавиатуре. 21 пользователь набирают свои пароли с длиной от 6 до 10 символов, генерируя нормальный класс данных и 15 «злоумышленников» симулируют потенциальные попытки вторжения, используя пароли 21 пользователя. В общем 21 набор данных сконструирован для 21 пароля. Для каждого пользовательского пароля были собраны от 76 до 388 нормальных образцов для обучения и 75 для тестирования, а также были собраны 75 новых образцов. Если предположить, что учебный набор должен быть максимально несбалансированным, 50 пользовательских образцов и 5 образцов злоумышленников пробовались для обучения случайно. 75 нормальных образцов и оставшиеся 70 новых образцов составили тестовый набор. В конечном итоге, 30 различных обучающих тестовых наборов пробовались случайно для каждого пароля для уменьшения влияния образцов.

Были применены в общем 6 детекторов новизны, включая SVDD и 1-LVQ. Остальными моделями были Гауссов метод, метод Парзена, автоассоциативные нейронные сети (AANN), и одноклассовый метод опорных векторов (1-SVM), которые не могут использовать образцы злоумышленника, даже если они доступны.

В качестве оценки точности и надежности была выбрана интегральная ошибка EER (Equal Error Rates – совпадение вероятностей FAR и FRR), которая получена из ROC-кривой (Receiver Operating Characteristic) с уровнем от 0 до 50%.

В данном случае интерес представляет эффективность использования образцов злоумышленника. Для каждого пароля SVDD и 1-LVQ были обучены с двумя видами обучающих наборов, данных: один набор – с использованием образцов клавиатурного почерка и авторизованных пользователей, и злоумышленников, другой – с использованием только образцов зарегистрированных пользователей. Средняя интегральная ошибка для 21 пароля представлена в табл. 1. Для 16 из 21 пароля 1-LVQ, обученный с двумя наборами данных, показал лучший результат и в этих случаях интегральная ошибка была ниже на 10%. Для трех паролей: «autumnman», «dusru427», «yuhwalkk» обе модели достигли минимальной ошибки в 0%. В тоже время 1-LVQ, обученный только на наборе образцов зарегистрированных пользователей, никогда не показывал низшего значения интегральной ошибки. SVDD, обученный с двумя наборами данных, показал низкий уровено интегральной ошибки только для четырех паролей. Табл. 1 наглядно показывает, что с использованием образцов злоумышленника 1-LVQ показал гораздо лучшие результаты, чем SVDD. Интегральная ошибка шести моделей для 21 пароля представлена в табл. 1.

В данной таблице столбцы, обозначенные как «Both» и «normal» для 1-LVQ и SVDD указывают соответственно модели обучения с двумя наборами образцов и только с использованием образцов истинных пользователей. Жирным шрифтом выделено низшее значение ошибки для каждого пароля. Символ «*» указывает на лучшую модель.

Выводы

Были исследованы два детектора новизны для идентификации пользователей компьютерных систем по клавиатурному почерку. Если образцы злоумышленников недоступны вначале обучения, они могут быть доступны в дальнейшем после неудавшихся попыток вторжения. Было предложено переобучить детектор новизны 1-LVQ и SVDD с использованием образцов злоумышленников. Экспериментальные данные на 21 образце клавиатурного почерка продемонстрировали, что 1-LVQ, переобученный с использованием образцов злоумышленников, дает преимущества в сравнении с другими методами, хотя результаты, которые показал метод SVDD, были не столь значительны. В сравнении с другими широко известными детекторами новизны 1-LVQ показал в результате значительно низший уровень интегральной ошибки.

Дополнительно хотелось бы обратить внимание на некоторые моменты. Во-первых, в данной статье не рассматривалась проблема выбора пара-

Таблица 1

Средняя интегральная ошибка (%) для шести детекторов новизны

Пароль	1-LVQ		SVDD		Gauss	Parzen	AANN	1-SVM
	Both	Normal	Both	Normal				
90200jdg	1.88	2.15	1.97	1.97	**1.58***	2.66	3.43	1.91
ahrfus88	**0.33***	0.46	0.50	0.50	0.73	0.59	0.77	0.48
anehwksu	0.28	0.38	0.33	0.33	**0.16***	0.43	1.46	0.30
autumnman	0.00	0.00	0.00	0.00	0.00	0.00	0.40	0.00
beaupowe	0.02	0.02	0.01	0.01	0.01	0.02	0.81	0.01
c.s.93/ksy	**0.14***	0.19	0.19	0.19	0.82	0.22	0.23	0.19
dhfpql.	**0.71***	0.89	0.86	0.87	0.85	1.12	1.99	0.80
dirdhfmw	**0.37***	0.83	0.96	0.96	1.30	1.37	2.13	0.87
dlfjs wp	**0.42***	0.45	0.45	0.45	0.49	0.50	2.26	0.45
dltjdgml	0.00	0.00	0.00	0.00	0.02	0.00	0.17	0.00
drizzle	**0.06**	0.10	0.09	0.09	0.26	0.18	0.74	0.08
dusru427	0.00	0.00	0.00	0.00	0.00	0.00	0.02	0.00
i love 3	**0.86**	1.04	1.13	1.14	0.87	1.22	2.68	1.05
love wjd	**0.85***	1.39	1.70	1.72	2.24	2.14	3.38	1.59
loveis.	**0.32***	0.44	0.42	0.42	0.93	0.50	0.98	0.41
manseiii	**0.59***	1.02	1.19	1.20	2.45	1.46	1.94	1.08
rhkdwo	**0.77***	1.32	1.45	1.45	1.58	2.23	2.66	1.38
rla sua	0.01	0.03	0.01	0.01	0.06	0.06	0.38	0.01
tjddmswjd	**0.24***	0.38	0.46	0.46	1.23	0.96	2.31	0.40
tmdwnsl1	**1.13***	1.18	1.22	1.22	1.36	1.32	2.07	1.20
yuhwa1kk	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Общее среднее	**0.43**	0.59	0.62	0.62	0.81	0.81	1.47	0.58

метров клавиатурного почерка. На практике специфический набор параметров должен быть определен заранее. Хотелось бы отметить, что достаточно сложно отобрать соответствующие параметры, приемлемые одновременно для обоих методов: 1-LVQ и SVDD. Во-вторых, исследовались 5 образцов злоумышленников. Необходимо дополнительно исследовать, какое количество образцов злоумышленников необходимо для 1-LVQ и для SVDD. В-третьих, при проведении эксперимента использовались все особенности клавиатурного почерка для обучения. Однако общеизвестно, что некоторые характеристики являются более весомыми, в то время как другие оказываются незначительными или даже бесполезными. Таким образом, удачная схема отбора особенностей и характеристик клавиатурного почерка может улучшить точность. Невзирая на указанные ограничения, можно с уверенностью констатировать, что использование образцов злоумышленника для переобучения детектора новизны, использующего метод 1-LVQ, целесообразно и эффективно.

Список литературы

1. R. Spillane, "Keyboard Apparatus for Personal Identification", IBM Technical Disclosure Bulletin, vol. 17, no. 3346, 1975.

2. G. Forsen, M. Nelson, and R. Staron, Jr. "Personal attributes authentication techniques", Technical Report RADC-TR-77-333, Rome Air Development Center, October 1977.

3. R. Gaines, W. Lisowski, S. Press, and N. Shapiro, "Authentication by keystroke timing: some preliminary results", Rand Rep. R-2560-NSF, Rand Corporation, 1980.

4. Lawrence O'Gorman. Comparing Passwords, Tokens, and Biometrics for User Authentication. Proceedings of the IEEE, Vol. 91, No. 12, Dec, pp. 2019-2040, 2003.

5. Salil P. Banerjee, Damon L. Woodard. Biometric Authentication and Identification using Keystroke Dynamics: A Survey // Journal of Pattern Recognition Research 7 (2012). – P. 116-139.

6. Иванов А.И. Нейросетевые алгоритмы биометрической идентификации личности. Кн. 15: Монография / А.И. Иванов. – М.: Радиотехника, 2004. – 144 с.

7. Mrs. D. Shanmugapriya, Dr. G. Padmavathi. A Survey of Biometric keystroke Dynamics: Approaches, Security and Challenges // International Journal of Computer Science and Information Security, Vol. 5, No. 1, 2009. – P. 115-119.

8. Hyoung-joo Lee, Sungzoon Cho. The novelty detection approach for different degrees of class imbalance // Lecture Notes in Computer Science Volume 3832, 2005. – P. 633-639.

9. Hyoun-joo Lee, Sungzoon Cho. Retraining a Novelty Detector with Impostor Patterns for Keystroke Dynamics-Based Authentication // ICB, vol. 3832 of Lecture Notes in Computer Science, 2006. – P. 633-639,.

10. Hyoun-joo Lee, Sungzoon Cho. Retraining a keystroke dynamicsbased authenticator with impostor patterns // Computers & Security, 2007, .vol. 26, no. 4. – P. 300-310,

11. Cho S., Han C., Han D., Kim H.:Web Based Keystroke Dynamics Identity Verification using Neural Networks. Journal of Organizational Computing and Electronic Commerce 10(4) (2000). – P. 295-307.

12. Yu E., Cho S.: Keystroke Dynamics Identity Verification - Its Problems and Practical Solutions. Computer and Security 23(5) (2004). – P. 428-440.

13. Schölkopf B., Platt J.C., Shawe-Taylor J., Smola A.J., Williamson R.C. Estimating the Support of a High-dimensional Distribution. Neural Comp. 13 (2001). – P. 1443-1471.

14. Tax D.M.J., Duin R.P.W. Support Vector Data Description. Machine Learning 54 (2004). – P.45-66.

15. Lee H., Cho S. SOM-based Novelty Detection Using Novel Data // Proc.of Sixth International Conference on Intelligent Data Engineering and Automated Learning, Lecture Notes in Computer Science 3578 (2005). – P. 359-366.

Поступила в редколлегию 22.05.2014

Рецензент: д-р ф.-м. наук, проф. М.Г. Любарський, Национальный юридический университет им. Я. Мудрого, Харьков.

ПІДХІД ДО ПІДВИЩЕННЯ НАДІЙНОСТІ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ КОМП'ЮТЕРНИХ СИСТЕМ ЗА ДИНАМІКОЮ НАПИСАННЯ ПАРОЛІВ

Н.А. Кошева, Н.І. Мазниченко

Проаналізовані можливості ідентифікації користувача по особливостях клавіатурного почерку, які використовуються в системах контролю і управління доступом до інформаційних комп'ютерних систем. Розглянуті підходи по підвищенню надійності даного методу ідентифікації.

***Ключові слова**: клавіатурний почерк, ідентифікація користувачів ЕОМ.*

APPROACH TO INCREASE OF RELIABILITY OF AUTHENTICATION OF USERS OF COMPUTER SYSTEMS ON DYNAMICS OF WRITING OF PASSWORDS

N.A. Koshevaya, N.I. Maznichenko

Possibilities of user identification on the features of keyboard handwriting, which are used in the checking systems and management by access to the informative computer systems, are analysed. Approaches on the increase of reliability of this method of authentication are considered.

***Keywords:** keystroke dynamics, computer user identification.*