АВЕРИН А. И., СИДОРОВ Д. П.

АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ ПО КЛАВИАТУРНОМУ ПОЧЕРКУ

Аннотация. В связи с бурным развитием сетевых технологий и повсеместным внедрением многопользовательских компьютерных систем особую актуальность приобрела задача аутентификации пользователя в такой системе. В статье рассмотрены возможные способы аутентификации. Подробно рассмотрена возможность аутентификации пользователя путем анализа его клавиатурного почерка.

Ключевые слова: защита информации, пароль, биометрическая аутентификация, клавиатурный почерк.

AVERIN A. I, SIDOROV D. P.

USER AUTHENTICATION BASED ON KEYSTROKE DYNAMICS

Abstract. Due to the rapid development of network technology and universal introduction of multi-user computer systems, the problem of user authentication has become particularly relevant. This article considers the user authentication methods with a focus on analyzing the keystroke dynamics.

Keywords: data security, password, biometric authentication, keystroke dynamics.

Одной из наиболее важных проблем современного общества, является защита личной информации от несанкционированного доступа. Миллиарды терабайт данных хранятся на компьютерах пользователей по всему миру. И эти данные могут иметь разную степень значимости: начиная от фотографий из личного цифрового альбома и заканчивая информацией, представляющей значительную коммерческую ценность.

Защита информации в компьютерных системах и сетях – это комплексная задача, решение которой происходит с помощью внедрения различных систем безопасности. Одну из главных ролей в решении данной задачи играет элемент обеспечивающий контроль доступа к ресурсам компьютерной системы. Такой элемент выполняет свои функции при помощи процедур идентификации и аутентификации пользователей. Эти процедуры являются основополагающими в любой системе защиты от несанкционированного доступа, потому что каждый пользователь должен быть однозначно определен и должно быть гарантировано соответствие пользователей с их идентификаторами, так как дальнейшая работа в системе ведется только с идентифицированными субъектами.

Для аутентификации система должна хранить информацию, которая характеризует неповторимые качества конкретного пользователя. Эта информация называется аутентификационной и в зависимости от ее типа различают парольный, имущественный и

биометрический методы аутентификации.

Классическим методом аутентификации пользователей является использование уникальной информации – пароля, который известен пользователю и который он предъявляет во время аутентификации [6]. Этот метод самый распространенный, так как он простой и дешевый с точки зрения реализации. Но наряду со всеми его достоинствами он обладает огромным недостатком. При нарушении конфиденциальности пароля полностью нарушается защита информации владельца.

Имущественный метод аутентификации основан на владении пользователем некоторым уникальным предметом (ключ, смарт-карта, токен), который он предъявляет системе. Данный метод имеет тот же недостаток, что и предыдущий: в случае утери или кражи аутентификационного предмета полностью нарушается защита информации. Кроме того, имущественный метод дороже в реализации, т.к. требуется специальное оборудование для распознавания предмета, используемого при аутентификации. Уникальные предметы также необходимо изготовить, что связано с некоторыми расходами.

Для устранения указанных недостатков при аутентификации можно использовать биометрические характеристики пользователя. Биометрия позволяет идентифицировать пользователей, опираясь на их поведенческие и физиологические характеристики. К физиологическим характеристикам можно отнести отпечатки пальцев, черты лица, геометрия ладоней, ушных раковин, сетчатка глаза и т. д. [4]. Поведенческие характеристики включают почерк человека, походку, тембр голоса, скорость набора текста на клавиатуре и т.п.

Если определение пользователя с помощью сканирования сетчатки глаза весьма дорогостоящий способ, в связи со стоимостью оборудования, то идентификация пользователя по клавиатурному почерку – дешевый и достаточно простой для реализации вариант, так как для такой системы не нужно дополнительного оборудования. Требуется стандартный набор периферийных устройств, которые имеет в своем распоряжении любой персональный компьютер – клавиатура и монитор. А в качестве системы безопасности будет выступать программный продукт, разработка которого и представляет основную сложность.

Так что же такое клавиатурный почерк? Одной из повседневных задач, решаемых людьми, является набор текстов на клавиатуре компьютера. В процессе того как человек вводит информацию используя клавиши у него вырабатывается свой личный стиль набора тех или иных слов. И этот стиль фактически не повторим и зависит от таких параметров как: количество пальцев, задействованных во время набора текста; длительность нажатия клавиш; время между нажатиями клавиш; использование основной или дополнительной части клавиатуры; характер сдвоенных или строенных нажатий; излюбленные сочетания горячих клавиш и т. д. Таким образом, клавиатурный почерк – это набор динамических характеристик

работы на клавиатуре.

Важной особенностью задачи аутентификации пользователя по клавиатурному почерку является необходимость «обучения» программы, которая будет производить аутентификацию. Под обучением понимается накопление информации, характеризующей особенности работы каждого пользователя с клавиатурой. Далее эта информация подвергается обработке [3].

Начальным этапом обработки данных является фильтрация. Входной поток данных преобразуется таким образом, чтобы он не содержал информацию о «служебных» клавишах – клавишах управления курсором, функциональных клавишах и т. п.

На следующем этапе выделяется информация, относящаяся к характеристикам пользователя, описанным в работе [1]:

- количество опечаток;
- время удержания клавиш;
- интервалы между нажатиями клавиш;
- число перекрытий между клавишами;
- скорость набора;
- степень аритмичности при наборе.

После статистической обработки этих данных рассчитанные эталонные характеристики пользователя сохраняются в базе данных.

При аутентификации, опознавание пользователя состоит в сравнении биометрической информации, которая будет получена при вводе текста с соответствующей этому пользователя эталонной информацией хранимой в памяти компьютера.

Аутентификация по клавиатурному почерку также не лишена недостатков – она не определяет пользователя с абсолютной точностью. Если с паролем все просто (совпадение или несовпадение с эталоном), то системы биометрической аутентификации распознают пользователя с определенной вероятностью. Так как биометрические характеристики прямо зависят от эмоционального состояния человека и условий, в которых он вводит кодовую фразу, система может не распознать легального пользователя, а в худшем случае предоставить доступ к закрытой информации человеку, которому она не предназначена.

Поэтому в системах биометрической аутентификации присутствуют две оценочные характеристики, приведенные в работе [2]:

1. отказ в доступе (false rejection rate, FRR – ошибка первого рода) – с какой вероятностью система не узнает зарегистрированного пользователя;
2. ложный доступ (false access rate, FAR – ошибка второго рода) – вероятность ошибочного допуска нелегального пользователя.

Отметим ряд некоторых интересных особенностей, выявленных на основе статистических данных.

Вероятность аутентификации пользователя по времени удержания клавиш в зависимости от длины ключевой фразы является более стабильной характеристикой клавиатурного почерка пользователя, чем время между нажатиями клавиш (пауз), которое и растет с ростом длины ключевой фразы. Это объясняется тем, что процесс нажатия клавиши на клавиатуре является истинно подсознательным процессом мышления.

Время между нажатиями клавиш является менее стабильной характеристикой клавиатурного почерка пользователя, чем время удержания клавиш. Функция вероятности идентификации от пауз между нажатиями клавиш имеет максимум своего значения при длине ключевой фразы порядка 810 символов. Это объясняется тем, что ключевые фразы небольшой длины, состоящие из одного, максимум двух слов, пользователь набирает подсознательно. Подсознательные движения стабильны до тех пор, пока в них не вмешивается более высокий сознательный уровень мышления, что приводит к появлению эффекта «сороконожки», сбивающейся при попытке понять, как же она ходит.

Проявление данного эффекта объясняет уменьшение вероятности аутентификации пользователя при превышении длины ключевой фразы некоторого критического уровня. Следует отметить, что значение данного порога достаточно сильно варьируется для пользователей с различным опытом работы с клавиатурой и может колебаться от 6 до 30 символов. После этого предела даже у квалифицированных машинисток наблюдается эффект включения сознательного мышления и остановок в наборе текста для принятия решения. В соответствии с изложенными выводами можно говорить о том, что в системах аутентификации пользователя по особенностям клавиатурного почерка не рекомендуется использовать слишком длинные выражения в качестве ключевой фразы, так как это приводит к тому, что пользователь начинает «осмысленно» выполнять набор текста, что может привести к снижению качества его аутентификации.

Подводя итог всему вышесказанному, систематизируем основные преимущества и недостатки аутентификации пользователей по клавиатурному почерку.

Преимущества.

- Простота реализации и внедрения. Реализация исключительно программная, ввод осуществляется со стандартного устройства ввода (клавиатуры), а значит – использование не требуется приобретение никакого дополнительного оборудования. Это самый дешевый способ аутентификации по биометрическим характеристикам субъекта доступа.
- Не требует от пользователя никаких дополнительных действий и навыков. Пользователь, так или иначе, наверняка использует пароль, который можно назначить парольной фразой,

по которой будет проводиться аутентификация. Возможно, мошеннику удастся получить логин и пароль для входа в систему, но вот скопировать клавиатурный почерк не представляется возможным.

- Возможность скрытой аутентификации – пользователь может не знать, что включена дополнительная проверка, а значит не сможет сообщить об этом злоумышленнику.

Недостатки.

- Требуется обучение приложения.
- Сильная зависимость от эргономичности клавиатуры (в случае замены клавиатуры придется обучать программу заново).
- Сильная зависимость от психофизического состояния оператора. Если человек заболел, то он вполне вероятно не сможет аутентифицироваться (с другой стороны, может и не стоит этого делать в больном состоянии).

В заключение добавим, что аутентификация лишь с использованием анализа клавиатурного почерка неприемлема в системах, требующих высокого уровня защиты. Но в сочетании с другими системами аутентификации может оказаться весьма эффективной.

Анализ существующей литературы по данному вопросу позволяет сделать вывод о том, что многие вопросы аутентификации пользователей на основе их клавиатурного почерка пока не изучены. Существующие программные реализации подобных систем характеризуются недостаточной достоверностью аутентификации. Актуальна разработка новых методов, алгоритмов и их программно-аппаратных реализаций, повышающих эффективность систем идентификации и аутентификации.

ЛИТЕРАТУРА

1. Ilonen J. Keystroke Dynamics [Электронный ресурс] // Lappeenranta University of Technology. – 2008. – Режим доступа: http://researchweb.iiit.ac.in/~vandana/ PAPERS/KS/Ilonen.pdf.
2. Checco J. C. Keystroke Dynamics and Corporate Security [Электронный ресурс] // WSTA Ticker Magazine. – 2003. – Режим доступа: http://www.checco.com/about/john.checco/ publications/2003_Keystroke_Biometrics_Intro.pdf.
3. Горелик А. Л., Скрипкин В. А. Методы распознавания. – М.: Высшая школа, 1984. – 80 с.
4. Задорожный В. Обзор биометрических технологий // Защита информации. Конфидент. – 2003. – № 5. – С. 26–29.
5. Сарбуков А. Е., Грушо А. А. Аутентификация в компьютерных системах // Системы безопасности. – 2003. – № 5(53). – С. 118–122.