ISSN 2411-1031. Information Technology and Security. January-June 2016. Vol. 4. Iss. 1 (6)

УДК 004.056.53

ВІКТОР ЄВЕЦЬКИЙ,
ІВАН ГОРНІЙЧУК

ВИКОРИСТАННЯ КЛАВІАТУРНОГО ПОЧЕРКУ В СИСТЕМАХ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧА

У статті коротко розглянуті питання використання біометричних характеристик для підвищення ефективності автентифікації користувача. Ідентифікатор, що використовує біометричні характеристики, нерозривно пов'язаний з користувачем, і скористатися ним несанкціоновано практично неможливо. Як біометричну характеристику доцільно використати клавіатурний почерк. Клавіатурний почерк, або ритм набору тексту, відображає спосіб набору тексту на клавіатурі, властивий тільки конкретному користувачеві. Крім того, він досить простий в реалізації і не вимагає додаткових апаратних витрат. Як ключовий текст доцільно використовувати пароль користувача. Тим більше, що використання клавіатурного почерку при введенні пароля усуває основні недоліки класичних парольних систем і систем на основі карт доступу. Наведено опис розробленої програми для практичного використання клавіатурного почерку. Програма крім прийняття рішень дозволяє проводити збір статистичного матеріалу для подальшого аналізу. Використання програми не завдає незручностей користувачеві.

Ключові слова: біометричні характеристики, автентифікація користувача, клавіатурний почерк, парольна автентифікація, програма допуску користувача.

Постановка проблеми. Для захисту комп'ютерної інформації використовуються системи управління доступом. При управлінні доступом процедури ідентифікації і автентифікації повинні гарантувати відповідність між користувачем і його ідентифікатором, що запобігає несанкціонованому доступові (НСД) до інформації. Завдяки простоті реалізації і використання найбільшого поширення набула парольна автентифікація. Однак, цей метод має істотний недолік, який полягає в тому, що в класичних парольних системах, а також системах на основі карт доступу підглядання або вгадування пароля, крадіжка або виготовлення дубліката картки призводить до компрометації всієї системи.

Для підвищення ефективності автентифікації доцільно використовувати додаткові характеристики, властиві тільки конкретному користувачеві. Системи, що використовують біометричні характеристики користувача практично позбавлені цих недоліків, так як ідентифікатор нерозривно пов'язаний з самим користувачем і скористатися ним несанкціоновано практично неможливо.

Аналіз останніх досліджень і публікацій. Клавіатурний почерк як біометрична характеристика відноситься до динамічних (поведінкових) характеристик, що описують підсвідомі дії, звичні для користувача. Клавіатурний почерк або ритм друкування, відображає спосіб друкування користувачем того чи іншого тексту. В якості унікальної інформації, властивої тому чи іншому користувачеві, можна відзначити наступні найбільш типові ознаки [1]:

- кількість помилок при наборі;
- інтервали між натисканнями клавіш;
- час утримання клавіш;
- число перекриттів між клавішами;
- ступінь аритмічності при наборі;
- швидкість набору.

Клавіатурний почерк можуть характеризувати й інші параметри, описані в ряді робіт: загальний час набору парольної фрази, частота виникнення помилок при наборі,

факт використання додаткових клавіш (використання числової клавіатури), особливості введення великих літер (використання клавіші Shift або Caps Lock) і т. д.

При цьому найбільш прості в реалізації наступні ознаки: тимчасові інтервали між натисканнями клавіш, час утримання клавіш і швидкість набору. Саме ці ознаки дозволяє без труднощів вимірювати стандартна клавіатура. Часові інтервали між натисканням клавіш на клавіатурі і час утримання (натискання) клавіш дозволяють досить однозначно характеризувати почерк роботи користувача на клавіатурі, що підтверджується рядом експериментів [2]. При наборі тексту на клавіатурі тимчасові інтервали між натисканням клавіш характеризують темп роботи, а час утримання клавіш характеризує стиль роботи з клавіатурою (різкий удар або плавне натискання). Використання клавіатурного почерку саме при наборі пароля дозволить, на нашу думку, суттєво посилити надійність автентифікації користувача.

З огляду на проведений аналіз останніх досліджень і публікацій [1-7], мета данної роботи полягала в розробці програми, яка відповідала б поставленим вимогам і забезпечувала би використання клавіатурного почерку при автентифікації користувача, а також мала можливість накопичення статистичного матеріалу для подальшого аналізу.

Виклад основного матеріалу дослідження. Слід зазначити, що використання клавіатурного почерку при введенні пароля не вимагає установки спеціальних апаратних засобів і не завдає незручностей. Крім того клавіатурний почерк дозволяє також проводити повторну автентифікацію для підтвердження особи користувача перед виконанням критичних операцій і, за необхідності, дозволяє проводити приховану автентифікацію.

При цьому, оскільки пароль крім виконання своєї основної функції ще є прикладом тексту, до нього висуваються і деякі додаткові вимоги: розташування використовуваних клавіш при наборі, довжина пароля і деякі інші.

При введенні пароля бажано (і навіть необхідно), щоб процес введення здійснювався практично підсвідомо, так як саме підсвідомі рухи стабільні для даного користувача і характеризують його стиль роботи з клавіатурою. Як свідчать результати роботи [2], поява усвідомленого рівня мислення при значному збільшенні довжини ключової фрази призводить до погіршення якості автентифікації користувача. Вищевикладене, на нашу думку, говорить про доцільність використовувати в якості ключового тексту пароль користувача довжиною 8-16 символів.

В роботі [3] наведені результати можливого підходу до оцінювання інформативності окремих ознак і різних їх сукупностей для цілей індивідуального розпізнавання. Для кількісного оцінювання можливостей окремих характеристик клавіатурного почерку і їх сукупностей для автентифікації користувача необхідний відповідний статистичний матеріал.

Практичне використання клавіатурного почерку для аутентифікації вимагає розробки програми, яка крім прийняття рішень дозволяла б проводити збір необхідного статистичного матеріалу. Аналіз отриманого статистичного матеріалу дозволить:

- оцінити інформативність окремих ознак та їх сукупностей для поставлених цілей;
- зробити висновки про стабільність в часі окремих ознак;
- оцінити вплив на якість роботи системи емоційного стану користувача, ступеня втоми та інших характеристик.

Для отримання достовірних результатів необхідний тривалий період роботи з програмою, так як при використанні непредставницьких вибірок можливе прийняття неправильних рішень.

Доцільно також зазначити, що при розробленні програми автентифікації користувача необхідно вжити заходи для захисту файлів з характеристиками користувача і самої програми від зловмисного втручання. Розроблена програма “Клавіатурний почерк” складається з двох підпрограм:

1. HandWriting.exe – це програма, що дозволяє створювати/видаляти користувачів, а також редагувати їх паролі (див. рис. 1).

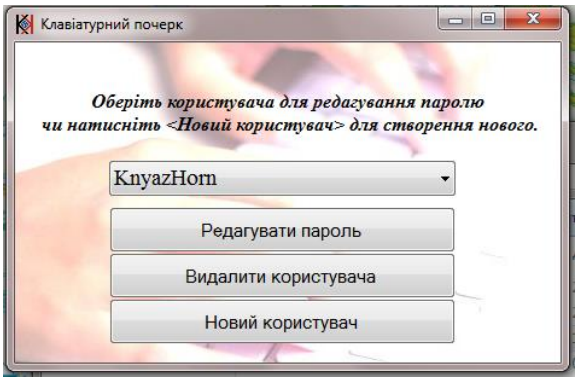

Рисунок 1 – Головне вікно програми HandWriting.exe

При створені/видалені користувача додається або видаляється відповідний запис в файлі ”Users/Users.ini”. При створені користувача і відповідно при його редагуванні, необхідно ввести пароль довжиною N літер, підтвердити його, далі відбувається ”вивчення” почерку.

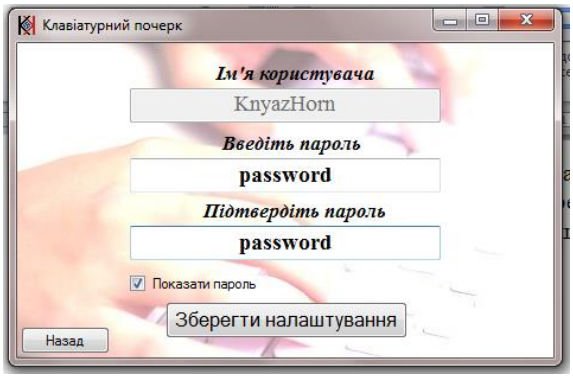

Рисунок 2 – Вікно редагування паролю програми HandWriting.exe

Пароль зберігається в ключі користувача, що знаходяться в файлі ”Users/<ім’я користувача>” в хешованому вигляді. Процедура вивчення почерку полягає в послідовному введені паролю 15 разів підряд. Під час введення паролю отримуємо часові характеристики кожного введення, що формують матрицю $v(15,n)$, $n=2N-1$. В цій матриці рядок $v_i=(t_{i,1},t_{i,2},t_{i,3},...,t_{i,n})$ – часовий вектор, $t_{i,j}$ – час утримання j-ої клавіші, що відповідає j-ій літері паролю, а $t_{i,2j}$ – інтервал між натисканням j-ої та $j+1$-ої клавіші. Перших 10 часових векторів використовуються для формування інтервалів ключа-шаблону користувача, а останні 5 – для вивчення максимально-допустимої кількості помилок, що можна припустити при введені паролю.

Для отримання часових інтервалів для $t_{i,j}$ візьмемо показники $(t_{1,j},t_{2,j},t_{3,j},...,t_{10,j})$, тобто часові характеристики для j-ого показника. Визначаємо математичне очікування для j-ого показника:

$$m_j=\frac{\sum_{i=1}^{10}t_{i,j}}{10}.$$

Визначаємо дисперсію для j-ого показника:

$$\sigma_j^2=\frac{\sum_{i=1}^{10}(t_{i,j}-m_j)^2}{10}.$$

Часовий інтервал $(t_{j\min};t_{j\max})$, тобто проміжок значень, які допускаються при введені паролю, формується наступним чином:

$$t_{j\min} = m_j - T[L,(1-p_i)]\cdot\sigma_j,$$
$$t_{j\max} = m_j + T[L,(1-p_i)]\cdot\sigma_j,$$

де m_j – математичне очікування j-ого показника;

$T[L,(1-p_i)]$ – коефіцієнт Стьюдента;

L – кількість використаних при виченні прикладів;

p_i – задане значення вірогідності помилок першого роду.

В конкретно нашому випадку $T[10,(1-0{,}01)] = 2{,}82$.

Після цього формується ключ-шаблон користувача – вектор інтервалів для часових показників:

$$V_{key} = (t_{1\min}, t_{1\max}, t_{2\min}, t_{2\max}, ..., t_{n\min}, t_{n\max}).$$

Для аналізу прийняття рішення про істинність користувача, будемо використовувати міру Хемінга, що являє собою вектор E з 0 та 1, де 0 – відповідають попаданню часової характеристики в часовий інтервал встановлений ключем-шаблоном, а 1 – непопаданню. В результаті для істинного користувача цей вектор складається переважно з 0.

Абсолютне значення відстані Хемінга e_a до біометричного ключа-шаблону визначається як загальна кількість невідповідностей біометричному еталону. Вона завжди додатня і змінюється від 0 до n.

Для використання такого підходу необхідно визначити максимальне абсолютне значення відстані Хемінга $e_{\max}$. Для цього необхідно проаналізувати останніх 5 часових векторів і знайти загальну кількість неспівпадань з ключем-шаблоном – e_{sum}, та e_i – кількість неспівпадань в i – ому часовому векторі.

$$m_в = \frac{\sum_{i=1}^{5} e_i}{5}$$
$$\sigma_в^2 = \frac{\sum_{i=1}^{5} (e_i - m_в)^2}{5}$$
$$e_{\max} = m_в + T[L,(1-p_i)]\cdot\sigma_в$$

В нашому конкретному випадку $T[5,(1-0{,}01)] = 3{,}75$.

Таким чином формується ключ-шаблон користувача, який буде збережений в файлі “Users/<ім’я користувача>”.

2. LogIn.exe – програма, що завантажується після старту операційної системи, зупиняє процес explorer.exe, і вимикає будь-яку програму, що намагається відкритись і отримати управління (див. рис. 2). При вдалій авторизації користувача програма повторно запускає процес explorer.exe.

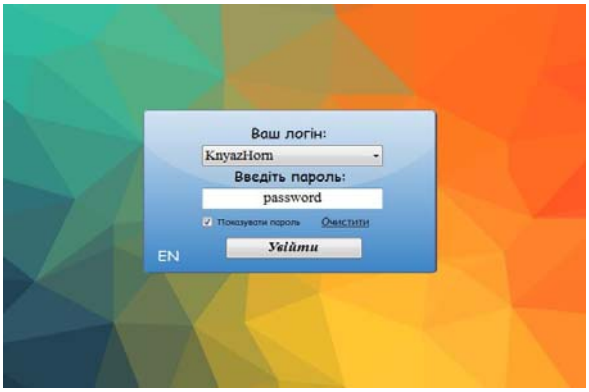

Рисунок 3 – Головне вікно програми LogIn.exe

Для входу необхідно ввести пароль, після чого він хешується і звіряється з паролем записаним в ключ-шаблон користувача, і якщо він правильний то перевіряються часові параметри авторизації, якщо кількість помилок допущених при введені менша за допустиму то програма визнає користувача істинним, і пропускає його до системи.

В програмі передбачено ведення журналу, в який заносяться і зберігаються: дата та час авторизації, логін, кількість помилок допущених при введені паролю, часові характеристики та результат авторизації. Журнал використовується для моніторингу надання доступу користувачам.

Висновки. Застосування біометричних характеристик дозволяє підвищити ефективність автентифікації користувача. Доцільність використання клавіатурного почерку, який властивий тільки конкретному користувачеві, полягає в тому, що він не потребує додаткових апаратних витрат і досить простий в реалізації. Як ключовий текст доцільно використовувати пароль.

Розроблена програма для практичного використання клавіатурного почерку при автентифікації користувача. Вона не завдає незручностей користувачеві. Крім прийняття рішень програма дозволяє проводити збір статистичного матеріалу і виконувати моніторінг надання доступу користувачам.

Перспективи подальших досліджень. Отримані за допомогою розробленої програми статистичні дані дозволять отримати ряд оцінок: інформативності окремих характеристик клавіатурного почерку і різних їх сукупностей, стабільності у часі характеристик клавіатурного почерку, впливу фізичного і емоційного стану користувача на характеристики його почерку.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] О.А. Коваленко, “Разработка системы анализа клавиатурного почерка”. [Электронный ресурс]. Доступно: http://elib.bsu.by/handle/123456789/7362. Дата обращения: Февр., 12, 2016.

[2] И.А. Ходашинский, М.В. Савчук, И.В. Горбунов, и Р.В. Мещеряков, “Технология усиленной аутентификации пользователей информационных процессов”, *Доклады ТУСУРа. Управление, вычислительная техника и информатика,* № 2 (24), с. 236-248, 2011.

[3] В.Л. Евецкий, “Оценка эффективности отдельных признаков и их совокупностей для индивидуального распознавания объектов”, *Information Technology and Security*, vol. 3, iss. 2, pp. 132-137, 2015.

[4] А.С. Калужин, и Д.Д. Рудер, “Подтверждение личности пользователя по его клавиатурному почерку”, *Известия Алтайского государственного университета*, т. 1, вып. 1 (85), с. 158-162, 2015.

[5] И.Г. Сидоркина, и А.Н. Савинов, “Три алгоритма управления доступом к ксии на основе распознавания клавиатурного почерка оператора”, *Вестник Чувашского университета*, № 3, с. 293-301, 2013.

[6] И. Агурьянов, “Клавиатурный почерк как средство аутентификации”. [Электронный ресурс]. Доступно: http://www.securitylab.ru/blog/personal/aguryanov/29985.php. Дата обращения: Февр., 12, 2016.

[7] В.Р. Григорьев, и А.П. Никитин, “Использование стастических методов для биометрической идентификации пользователя”, *Вестник РГГУ. Серия: Документоведение и архивоведение. Информатика. Защита информации и информационная безопасность*, № 14 (94), с. 135-143, 2012.

Стаття надійшла до редакції 06 березня 2016 року.

REFERENCE

[1] O.A. Kovalenko, “Developing of keyboard handwriting analysis system”. [Online]. Available: http://elib.bsu.by/handle/123456789/7362. Accessed on: Febr., 12, 2016.

[2] I.A. KHodashinskii, M.V. Savchuk, I.V. Gorbunov, and R.V. Meshcheriakov, “Strong authentication technology of the users of information processes”, *Proceedings of TUSUR University. Control systems, computers and computer science*, no. 2 (24), pp. 236-248, 2011.
[3] V.L. Yevetskyi, “Evaluation of certain signs and their collectively for individual recognition objects”, *Information Technology and Security*, vol. 3, iss. 2, pp. 132-137, 2015.
[4] A.S. Kaluzhin, and D.D. Ruder, “User Identity Confirmation with His Keystroke Pattern”, *Izvestiya of Altai State University*, vol. 1, iss. 1 (85), pp. 158-162, 2015.
[5] I.G. Sidorkina, and A.N. Savinov, “Three algorithms of control access to the ksii on the basis of recognition of keystroke dynamics”, *Bulletin of the Chuvash Universit*, no. 3, pp. 293-301, 2013.
[6] I. Agurianov, “Keyboard handwriting as tool of authentication”. [Online]. Available: http://www.securitylab.ru/blog/personal/aguryanov/29985.php. Accessed on: Febr., 12, 2016.
[7] V.R. Grigorev, and A.P. Nikitin, “Static methods for biometric user authentication”, *RGGU bulletin. Series: Records management and archive studies. Computer science. Data protection and information security*, no. 14 (94), pp. 135-143, 2012.

ВИКТОР ЕВЕЦКИЙ,
ИВАН ГОРНИЙЧУК

ИСПОЛЬЗОВАНИЕ КЛАВИАТУРНОГО ПОЧЕРКА В СИСТЕМАХ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ

В статье кратко рассмотрены вопросы использования биометрических характеристик для повышения эффективности аутентификации пользователя. Идентификатор, использующий биометрические характеристики, неразрывно связан с пользователем, и воспользоваться им несанкционированно практически невозможно. В качестве биометрической характеристики целесообразно использовать клавиатурный почерк. Клавиатурный почерк, или ритм набора текста, отображает способ набора текста на клавиатуре, свойственный только конкретному пользователю. Кроме того он достаточно прост в реализации и не требует дополнительных аппаратных затрат. В качестве ключевого текста целесообразно использовать пароль пользователя. Тем более, что использование клавиатурного почерка при вводе пароля устраняет основные недостатки классических парольных систем и систем на основе карт доступа. Приведено описание разработанной программы для практического использования клавиатурного почерка. Программа кроме принятия решений позволяет производить сбор статистического материала для последующего анализа. Использование программы не причиняет неудобств пользователю.

Ключевые слова: биометрические характеристики, аутентификация пользователя, клавиатурный почерк, парольная аутентификация, программа допуска пользователя.

VIKTOR YEVETSKYI,
IVAN HORNIICHUK

USE OF KEYBOARD HANDWRITING IN SYSTEMS OF THE USER AUTHENTICATION

Questions of biometric characteristics using for increase efficiency of user authentication are briefly considered in article. The identifier using biometric characteristics is inseparably linked with the user, and it is illegally almost impossible to use it. As biometric characteristics appropriate to use the keyboard handwriting. Keyboard handwriting, or a text typing rhythm, displays a text typing method on the keyboard, inherent only to the specific user. Furthermore it is quite simple to implement and requires no additional hardware costs. As a key text it is advisable to use a password. Moreover, the use of handwriting keyboard when entering your password eliminates the main disadvantages of the classic password systems and systems based on access cards. The description of the developed program for practical use of keyboard handwriting is given. The program except

decision making allows to make collecting of statistical material for the subsequent analysis. Use of the program does not cause inconveniences to the user. The program provides maintenance log, which records and stores the date and time of login, username, the number of errors made when entering the password, time and authorization result. The magazine is used for the monitoring of user access. The statistical data obtained by means of the developed program will allow to make number of estimates: informational content of separate characteristics of keyboard handwriting and their different sets, stability in time of characteristics of keyboard handwriting, influence of physical and emotional status of the user on characteristics of his handwriting and others.

Keywords: biometric characteristics, user authentication, keyboard handwriting, password authentication, program of the access permission of the user.

Віктор Леонідович Евецкий, кандидат технічних наук, доцент, доцент кафедри кібербезпеки та застосування автоматизованих інформаційних систем та технологій, Державний заклад "Інститут спеціального зв'язку та захисту інформації Національний технічний університет України "Київський політехнічний інститут", Київ, Україна.

E-mail**:** viktorevetsky@gmail.com.

Іван Вікторович Горнійчук, курсант, Державний заклад "Інститут спеціального зв'язку та захисту інформації Національний технічний університет України "Київський політехнічний інститут", Київ, Україна.

E-mail: knyazhorn@gmail.com.

Виктор Леонидович Евецкий, кандидат технических наук, доцент, доцент кафедры кибербезопасности и применения информационных систем и технологий, Государственное учреждение "Институт специальной связи и защиты информации Национального технического университета Украины "Киевский политехнический институт", Киев, Украина.

Иван Викторович Горнийчук, курсант, Государственное учреждение "Институт специальной связи и защиты информации Национального технического университета Украины "Киевский политехнический институт", Киев, Украина.

Viktor Yevetskyi, candidate of technical sciences, associate professor, associate professor at the cybersecurity and application of information systems and technologies academic department, State institution "Institute of special communication and information protection of National technical university of Ukraine "Kyiv polytechnic institute", Kyiv, Ukraine.

Ivan Horniichuk, cadet, State institution "Institute of special communication and information protection of National technical university of Ukraine "Kyiv polytechnic institute", Kyiv, Ukraine.

UDC 004.056.53

VITALII BEZSHTANKO,
OLEKSANDR MAKAREVYCH

IMPLEMENTATION OF INFORMATION SECURITY MANAGEMENT SYSTEM IN ORGANIZATION

The main objective of paper is the elaboration a common project of implementation information security management systems (ISMS) for organizations. For this, the steps of construction ISMS have been described in accordance with the rules and guidelines of the project management. Thus, in paper, the defined benefits were received by the company as a result of the implementation of an ISMS. The