УДК 004.056

ЗАСОБИ АУТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ КОМП'ЮТЕРНИХ СИСТЕМ НА ОСНОВІ ІНФОРМАЦІЙНИХ МОДЕЛЕЙ

Лигін Ю.О., Шумова Л.О.

MEANS FOR USER AUTHENTICATION IN COMPUTER SYSTEM BASED ON INFORMATION MODELS

Lyhin Y.O., Shumova L.O.

У статті розглянуто можливі способи аутентифікації користувачів у багатокористувальницьких комп'ютерних системах. Докладно розглянута можливість аутентифікації користувача шляхом аналізу його клавіатурного почерку, а саме досліджено алгоритм, який аналізує клавіатурний почерк після введення додаткового текстового фрагменту або фрази.

Ключові слова: *захист інформації, пароль, біометрична аутентифікація, клавіатурний почерк, парольна фраза.*

Вступ. Більше 20 років аутентифікація стоїть на першому рубежі контролю дозволеного доступу до інформації. Серед основних переваг захисту за допомогою аутентифікації можна відзначити її звичність і простоту. Проблеми аутентифікації розглядались у роботах таких вчених, як Гейнс (1980 р.) [1], Леггет і Вільямс [2], Расторгуєв [3], Сміт [4]. Класичним методом аутентифікації користувачів є використання унікальної інформації - пароля, який відомий користувачеві і який він пред'являє під час аутентифікації. Але за статистикою 80% інцидентів несанкціонованого доступу в сфері інформаційної безпеки трапляються внаслідок використання слабких паролів - до такого висновку прийшла компанія Trustwave за результатами власного дослідження, яке було проведене ще у 2011 році у ряді компаній у 18 регіонах світу. Головний висновок, зроблений в результаті: слабкі паролі користувачів - найбільш вразливе місце, яке використовують зловмисники.

Для створення пароля зазвичай ставиться безліч обмежень: певна кількість і склад символів, неможливість (небажаність) використання дат, слів, які можна знайти в словнику Застосування складних паролів призводить до їх недбалого зберігання у вигляді робочих записів, часто наочних, наприклад, у вигляді стікерів на робочому місці, тому зловмисникові не складе особливих труднощів отримати ці відомості. Виникає проблема такої аутентифікації, яка забезпечувала би більш надійний багаторівневий доступ до інформації, тобто крім пароля має використовуватись ще якийсь засіб, а може декілька засобів перевірки автентичності користувача.

Тому розробка засобів аутентифікації, що базуються на використанні особистих характеристик користувачів і забезпечують достатню точність, надійність, простоту реалізації є актуальними.

Постановка проблеми. Класичний метод доступу до інформації за допомогою пароля найпоширеніший. Він простий і дешевий в реалізації, але і більш ненадійний. При порушенні конфіденційності пароля повністю порушується захист інформації власника [5].

Ще один розповсюджений метод аутентифікації заснований на володінні користувачем деяким унікальним предметом (ключ, смарт-карта, токен), який він пред'являє системі. Даний метод має той же недолік, що і класичний: в разі втрати або крадіжки аутентифікаційного предмета повністю порушується захист інформації. Крім того, такий метод дорожче в реалізації, тому що потрібне спеціальне обладнання для розпізнавання предмета, використовуваного при аутентифікації. Унікальні предмети також необхідно виготовити, що пов'язано з деякими витратами [6].

Для усунення зазначених недоліків при аутентифікації можна використовувати біометричні характеристики користувача. Біометрія дозволяє ідентифікувати користувачів, спираючись на їх поведінкові і фізіологічні характеристики. До фізіологічних характеристик можна віднести відбитки пальців, риси обличчя, геометрію долонь, вушних раковин, сітківку ока і т.і. [7]. Поведінкові характеристики включають почерк людини, ходу, тембр голосу, швидкість набору тексту на клавіатурі [8]. Якщо визначення користувача за допомогою сканування сітківки ока досить дорогий спосіб, в зв'язку з вартістю обладнання, то ідентифікація користувача за клавіатурним почерком - дешевий і досить простий для реалізації варіант, так як для такої системи не потрібно додаткового обладнання.

Потрібен стандартний набір периферійних пристроїв, які має в своєму розпорядженні будь-який персональний комп'ютер - клавіатура і монітор. А в якості системи безпеки буде виступати програмний продукт, розробка якого і представляє основну складність. Аутентифікація за клавіатурним почерком - метод, що забезпечує високу в порівнянні з іншими методами точність, зручність застосування і неможливість відмови від факту авторства.

Існуючі програмні реалізації методів розпізнавання клавіатурного почерку характеризуються недостатньою достовірністю ідентифікації і аутентифікації і високою ймовірністю виникнення помилок першого і другого роду. Внаслідок цього актуальна розробка нових моделей, методів, алгоритмів розпізнавання клавіатурного почерку і їх програмних реалізацій, що підвищують точність і якість функціонування систем ідентифікації і аутентифікації.

Метою статті є визначення особливостей аутентифікації по біометричним параметрам особистості, а саме по клавіатурному почерку користувача при введенні ним парольних даних.

Для цього потрібно вирішити наступні задачі:

– провести аналіз особливостей введення користувачем коротких фраз;

– реалізувати методику фільтрації авторського введення від неавторського;

– запропонувати модель управління доступом з процедурою аутентифікації користувача.

Результати досліджень. На сьогоднішній день існує три алгоритму біометричної аутентифікації за клавіатурним почерком:

– алгоритм, що аналізує клавіатурний почерк під час введення паролю;

– алгоритм, що аналізує клавіатурний почерк після введення додаткового текстового фрагмента або фрази;

– алгоритм, який постійно проводить прихований моніторинг клавіатурного почерку користувача [9].

Перший алгоритм має найбільш високу швидкодією в порівнянні з іншими алгоритмами, тому що для отримання біометричних даних користувачеві необхідно ввести тільки пароль. Але не можна дати гарантію в точності аутетифікації, якщо пароль занадто короткий. Зазвичай пароль складається з 10-30 символів. Крім того, неможливо виявити підміну користувача в разі, якщо користувач пройшов аутентифікацію в системі і залишив робоче місце без нагляду, в той час як зловмисник зайняв його місце для корисливих цілей. З цих причин потрібні додаткові засоби перевірки автентичності користувача.

Другий алгоритм, який аналізує клавіатурний почерк після введення додаткового текстового фрагмента або фрази, в свою чергу, має перевагу перед першим алгоритмом у вигляді високої точності аутентифікації [10]. Але для введення додаткової фрази або текстового фрагмента, довжина яких часто перевищує 1000 символів, потрібно досить багато часу. Також ця процедура може викликати у користувача негатив через можливе часте проходження процедури аутентифікації з введенням довгого фрагмента тексту.

Для роботи даного алгоритму необхідно застосування ймовірнісно-статистичного методу, тобто збір статистики з вибірки тимчасових значень. Безпосередньо елементом вибірки є час утримання клавіші. Еталонна модель користувача створюється в режимі навчання. В цьому режимі збираються статистичні дані про натискання кожної клавіші. В результаті формується тривимірна таблиця, що складається з N стовпців, де N - кількість натиснутих клавіш (табл. 1).

Також визначається кінцеве число натискань певної клавіші k, де k - кількість натискань, дані про які необхідно створити для еталонної моделі. Таке число буде відображати кількість рядків в таблиці. У кожну клітинку таблиці буде заноситися значення про час утримання конкретної клавіші в певний момент натискання.

Таблиця 1

Збір статистичних даних

Клавіша 1	…	Клавіша N
Час 1-го утримання клавіші	…	Час 1-го утримання клавіші
…	…	…
Час k-го утримання клавіші	…	Час k-го утримання клавіші

Після збору всіх даних підраховується математичне сподівання кожної вибірки (для кожної клавіші), і еталон зберігається в обліковому записі.

Перед аутентифікацією користувач ідентифікує себе, тобто вводить пароль. Після цього проходить аутентифікацію. Користувачеві надається певний або випадковий текстовий фрагмент, довжина якого зазвичай може становити до 5000 символів. По ходу введення користувачем даного йому фрагмента, програма зчитує статистичні дані та порівнює їх з збереженими еталонними значеннями математичних сподівань різних вибірок.

Розглянемо більш докладно алгоритм біометричної аутентифікації, який аналізує клавіатурний почерк під час введення пароля. Даний алгоритм використовує при наборі на клавіатурі парольної фрази наступні біометричні характеристики: час натискання (td_i) і час віджимання (tu_i) клавіші, $i = 1,\ldots,n$, де n - довжина парольної фрази, і - повний час набору парольної фрази T.

За даними параметрами формується вектор біометричних параметрів V. Для створення еталонної моделі користувача необхідно 30 векторів V, тобто користувач повинен 30 разів ввести

парольну фразу. Після аналізу наявних 30 реалізацій вектора біометричних параметрів формуються інтервали допустимих значень для кожного параметра, які записуються в системі як еталонні для кожного користувача.

Далі відбувається другий етап реєстрації користувача - тестування системи. На даному етапі користувач повторно вводить парольну фразу 10 разів. І тепер система перевіряє параметр кожного вектора на потрапляння в еталонний інтервал. Для даного завдання і для кожного вектора біометричних параметрів створюється вектор E, який складається з нулів і одиниць. Якщо параметр потрапляє в еталонний інтервал, в вектор записується 0, інакше - 1.

Припустимо, що існує найкращий вектор E^*, який складається з одних нулів. Такий вектор передбачає потрапляння кожного параметра в свій інтервал. Тепер, щоб визначити, як відрізняти легітимного користувача від нелегітимного, введемо поняття граничного значення помилок при аутентифікації, тобто значення, що визначає, скільки разів параметр отриманого вектора не потрапить в інтервал еталонних значень. Для визначення порогового значення необхідно ввести відстань Хеммінга P між найкращим вектором і вектором тестового вектора біометричних параметрів. Таких відстаней в результаті буде 10. Далі, використовуючи отримані 10 відстаней Хеммінга, знаходимо математичне сподівання значення Хеммінга P, яке і буде граничним значенням, тобто дане число буде відображати допустиму кількість розбіжностей з біометричним еталоном, тобто з характерними інтервалами можливих значень параметрів.

При аутентифікації користувач вводить парольну фразу, тобто надає системі вектор біометричних параметрів. З цього вектору також формується вектор E і знаходиться його відстань Хеммінга від найкращого вектора E^*. Щоб визначити, легітимний це користувач чи ні, система порівнює отримане значення з пороговим, яке зберігається в системі. Процес прийняття рішення можна відобразити в наступній системі:

$$\begin{cases} E \le E^*, \text{користувач} - \text{Свій}; \\ \text{інакше, користувач} - \text{Чужий}. \end{cases}$$

Висновок. Проведений аналіз засобів аутентифікації показує, що біометричну аутентифікацію за клавіатурним почерком можна вважати достатньо прийнятною з позицій надійності, точності, простоти алгоритму реалізації. Розглянутий алгоритм такого засобу аутентифікації дозволить досягти прийнятного рівня помилок першого і другого роду при аутентифікації користувачів при малій кількості вимірювань і дасть можливість скоротити час як на створення шаблону клавіатурного почерку, так і на процедуру авторизації.

Література

1. R. Gaines, W. Lisowski, S. Press, and N. Shapiro. Authentication by Keystroke Timing: Some Preliminary Results," Rand Report R-256-NSF, Rand Corporation, Santa Monica, C A, 1980.
2. J. Leggett and Williams Verifying identity via keystroke characteristics // International Journal of Man-Machine Studies, 28:67-76, 1988.
3. Расторгуев С. П. Цель как криптограмма: криптоанализ синтетических целей (монография и два варианта пролегоменов к теории) / С. П. Расторгуев, В. Н. Чибисов – М.: Изд-во Агентства "Яхтсмен" – 1996.
4. Смит Р. Э. Аутентификация: от паролей до открытых ключей. − М.: Изд. дом «Вильямс», 2002. – 432 с.
5. Афанасьев А.А., Веденьев Л.Т., Воронцов А.А. и др. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. – М.: НТИ «Горячая линия – Телеком», 2012. - 550 с.
6. Ilonen J. Keystroke Dynamics [Електронний ресурс] // Lappeenranta University of Technology. - 2008. http://researchweb.iiit.ac.in/vandana/PAPERS/KS/Ilonen.pdf.
7. Горелик А. Л., Скрипкин В. А. Методы распознавания. - М .: Высшая школа, 1984. - 80 с.
8. Задорожний В. Обзор биометрических технологий // Защита информации. - М.: Конфидент. - 2003. - № 5. - С. 26-29.
9. Бідюк П., Бондарчук В. Сучасні методи біометричної ідентифікації [Електронний ресурс] Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, 1(18) вип., 2009 р. http://ela.kpi.ua/bitstream/123456789/9839/1/26.pdf
10. Сарбуков А.Е. Аутентификация в компьютерных системах / А.Е. Сарбуков, А.А. Грушо // Системы безопасности. – 2003. – № 5(53). – С. 118– 122.

References

1. R. Gaines, W. Lisowski, S. Press, and N. Shapiro. Authentication by Keystroke Timing: Some Preliminary Results," Rand Report R-256-NSF, Rand Corporation, Santa Monica, C A, 1980.
2. J. Leggett and Williams Verifying identity via keystroke characteristics // International Journal of Man-Machine Studies, 28:67-76, 1988.
3. Rastorguev S.P. Purpose as a cryptogram: cryptanalysis of synthetic targets (monograph and two variants of pro-domains to the theory) / S.P. Rastorguev, V.N. Chibisov - Moscow: Yachtsman Agency Publishing House - 1996.
4. Smith R. E. Authentication: from passwords to public keys. - M .: Izd. House "Williams", 2002. - 432 p.
5. Afanasyev A.A., Vedenev L.T., Vorontsov A.A. and others. Authentication. Theory and practice of providing secure access to information resources. - Moscow: NTI "Hot line - Telecom", 2012. - 550 p.
6. Ilonen J. Keystroke Dynamics [Electronic resource] // Lappeenranta University of Technology. - 2008. http://researchweb.iiit.ac.in/vandana/PAPERS/KS/Ilonen.pdf
7. Gorelik A. L., Skripkin V. A. Methods of recognition. - M.: Higher School, 1984. - 80 p.
8. Zadorozhnij V. Biometric Technologies Overview // Information protection. -M.: Konfident, - 2003. - № 5. - P. 26-29.
9. Bidyuk P., Bondarchuk V. Modern methods of biometric identification [Electronic resource] Legal, normative and metrological provision of information security system in

Ukraine, 1 (18) issue, 2009. http://ela.kpi.ua/bitstream/123456789/9839/1/26.pdf
10. Sarbukov A.E. Authentication in computer systems / A.E. Sarbukov, A.A. Grusho // Security Systems. - 2003.- No.5(53). - P. 118- 122.

Лыгин Ю.А., Шумова Л.А. Средства аутентификации пользователей компьютерных систем на основе информационных моделей.

В статье рассмотрены возможные способы аутентификации пользователей в многопользовательских компьютерных системах. Подробно рассмотрена возможность аутентификации пользователя путем анализа его клавиатурного почерка, а именно исследован алгоритм, который анализирует клавиатурный почерк после введения дополнительного текстового фрагмента или фразы.

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

Lyhin Y., Shumova L. Means for user authentication in computer system based on information models

The article considers possible ways of authentication of users in multi-user computer systems. The possibility of user's authentication by analyzing his keyboard handwriting is considered in detail, namely, an algorithm that analyzes the keyboard writing after the introduction of an additional text fragment or phrase is investigated.

Keywords: *information protection, password, biometric authentication, keyboard writing, passphrase.*

Лигін Ю.О. – магістрант кафедри комп'ютерних наук та інженерії Східноукраїнського національного університету імені Володимира Даля, e-mail: krauser15021992@gmail.com
Шумова Л.О. – к.т.н., доцент кафедри комп'ютерних наук та інженерії Східноукраїнського національного університету ім. В.Даля, e-mail: shumova@ukr.net

Рецензент: д.т.н., проф. ***Соколов В.І.***

Стаття подана 30.10.2018