УДК 681.3

Мазниченко Наталя Іванівна
Національний юридичний університет ім. Ярослава Мудрого
(Харків, Україна)

ПОСИЛЕНА ІДЕНТИФІКАЦІЯ І АУТЕНТИФІКАЦІЯ КОРИСТУВАЧА КОМП'ЮТЕРНИХ СИСТЕМ НА ОСНОВІ КЛАВІАТУРНОГО ПОЧЕРКУ

Анотація. *Проаналізовані можливості ідентифікації та аутентифікації користувача по особливостях клавіатурного почерку під час введення паролю, які використовуються в системах контролю і управління доступом до інформаційних комп'ютерних систем. Розглянуті переваги та недоліки даного методу.*

Ключові слова: *клавіатурний почерк, ідентифікація, аутентіфікація, захист інформації.*

Мазниченко Наталья Ивановна
Национальный юридический университет имени Ярослава Мудрого
(Харьков, Украина)

УСИЛЕННАЯ ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЯ КОМПЬЮТЕРНЫХ СИСТЕМ НА ОСНОВЕ КЛАВИАТУРНОГО ПОЧЕРКА

Аннотация. *Проанализированы возможности идентификации и аутентификации пользователя по особенностям клавиатурного почерка во время ввода пароля, которые используются в системах контроля и управления доступом к информационным компьютерным системам. Рассмотрены преимущества и недостатки данного метода.*

Ключевые слова: *клавиатурный почерк, идентификация, аутентификация, защита информации*

Maznichenko Natalia
National Law University named after Yaroslav the Wise
(Kharkiv, Ukraine)

INCREASE IDENTIFICATION AND AUTHENTICATION OF USER OF THE COMPUTER SYSTEMS ON THE BASIS OF THE KEYSTROKE DYNAMICS

Abstract. *Possibilities of user identification and authentication on the features of keyboard handwriting during the input of password, which are used in the checking systems and management by access to the informative computer systems, are analyses. Advantages and lacks of this method are considered*

Keywords: *keystroke dynamics, identification, authentication, data security.*

Постановка проблеми. У наш час загальній інформатизації особливу важливість і значущість набувають завдання захисту інформації, які пов'язані із забезпеченням безпечного збереження і конфіденційності інформації, що оброблюється та зберігається в комп'ютерних системах. Захист інформації в

комп'ютерних системах і мережах - це комплексне завдання, рішення якого відбувається за допомогою впровадження різних систем безпеки.

Важливою проблемою забезпечення безпеки інформаційних комп'ютерних систем є завдання обмеження кола осіб, що мають доступ до конкретної інформації і захисту її від несанкціонованого доступу.

Одним з головних елементів будь-якої системи захисту від несанкціонованого доступу (НСД) є елемент, що забезпечує контроль доступу до комп'ютерних системи і контроль роботи в них. Цей елемент захисту виконує свої функції за допомогою процедур ідентифікації і аутентифікації користувачів. Ці процедури важливі, тому що будь-якій системі захисту від НСД для виконання свого завдання необхідно, щоб усі легальні користувачі були ідентифіковані і гарантувалася б відповідність між користувачами і їх ідентифікаторами, оскільки усі інші елементи системи захисту працюють з ідентифікованими суб'єктами.

Система захисту виконує ідентифікацію та аутентифікацію на основі певної унікальної інформації, яка характеризує конкретного користувача системи.

Сьогодні використовуються наступні способи ідентифікації та аутентифікації користувачів [1, с. 216]:

1) парольний метод – використовує унікальне знання (наприклад, логін-пароль);

2) апаратний (або електронний) метод – використовує унікальний предмет (проксіміті-карти, смарт-карти, магнітні карти, токени і т.д.);

3) біометричний метод – використовує унікальні характеристики людини (відбитки пальців, сітківка ока, голос, почерк і т.д.).

Окремо слід відзначити комплексні методи ідентифікації/аутентифікації користувачів, які для цієї процедури використовують декілька ознак, що однозначно відповідають певній особі.

Парольний і апаратний методи мають деякі недоліки, головним з них є факт того, що є можливість обману/злому системи, крадіжки ключа, імітації унікального предмета, визначення або крадіжка паролю і т.д. Методи ідентифікації та аутентифікації за біометричними параметрами особи, зважаючи на невід'ємність біометричних характеристик конкретної людини, здатні забезпечити підвищену точність [2, с. 3]. До таких характеристик відноситься і клавіатурний почерк. Слід відзначити, що біометричні способи ідентифікації зазвичай потребують додаткових достатньо коштовних пристроїв. Також біометричні системи можна також обманути за допомогою муляжів відбитків пальців, фотографій, аудіо записів голосу і т.д. Тому останнім часом виникає гостра потреба в нових ідеях по управлінню доступом.

Виклад основного матеріалу. Підвищення точності та надійності систем ідентифікації та аутентифікації користувачів, на мій погляд, можна досягнути комбінуванням парольного захисту і біометричної ознаки. Нас цікавитиме в першу чергу поєднання захисту за допомогою пароля і за допомогою аналізу клавіатурного почерку (КП) користувача. Спробую обґрунтувати власну думку щодо доцільності та вдалості саме такої комбінації ідентифікаційних ознак, що визначають користувача комп'ютерної системи.

Парольні системи контролю і управління доступом є самими часто використовуваними засобами захисту комп'ютерної інформації на сьогоднішній

день [3, с. 14]. І цьому є логічне пояснення. Справа в тому, що парольна ідентифікація найбільш проста як у реалізації, так й у використанні. Крім того, введення парольної ідентифікації не вимагає зовсім ніяких витрат: даний процес реалізований у більшості програмних продуктів. Таким чином, система захисту інформації виявляється простою і доступною. Паролі давно вбудовані в операційні системи та інші сервіси. При правильному використанні паролі можуть забезпечити прийнятний для багатьох організацій рівень безпеки. Проте, по сукупності характеристик їх слід визнати найслабкішим засобом перевірки достовірності. Саме слабкий рівень парольного захисту є однією з основних причин уразливості комп'ютерних систем до спроб НСД. Тому ідея комбінації стандартного парольного захисту з методом ідентифікації/аутентифікації користувача по клавіатурному почерку представляється дуже вдалою. В ситуації, якщо зловмисник яким-небудь чином отримує доступ до пароля, доступ до комп'ютерної системи може бути заборонений завдяки ідентифікації по клавіатурному почерку, що проілюстровано на рис. 1. В даному випадку структура ідентифікації наступна: якщо користувач вводить некоректний пароль, йому вмить відмовляється в доступі. Якщо ж представлений коректний пароль, зразок клавіатурного почерку цього користувача зіставляється із зареєстрованими зразками авторизованих користувачів. Залежно від необхідної точності при зіставленні користувачеві може бути дозволений або заборонений доступ.

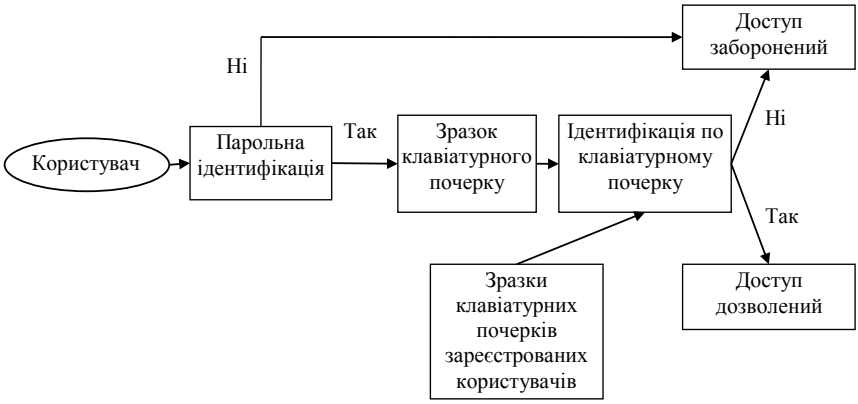

Рис. 1. Узагальнена структурна схема ідентифікації користувача по клавіатурному почерку під час введення паролю.

Методи ідентифікації та аутентифікації по клавіатурному почерку здатні забезпечити зручність для операторів автоматизованих комп’ютерних систем. Методи постійного прихованого клавіатурного моніторингу дозволяють виявляти підміну законного оператора і блокувати комп’ютерну систему від вторгнення зловмисника.

Проаналізувавши можливості використання клавіатурного почерку як індивідуальної ознаки для ідентифікації/аутентифікації користувачів під час

введення парольної фрази можна відзначити наступні переваги даного методу:

– простота реалізації і впровадження. Реалізація виключно програмна, введення здійснюється із стандартного пристрою введення (клавіатури), а це означає, що використання даного способу не потрібує придбання ніякого додаткового устаткування. Це найдешевший спосіб ідентифікації/аутентифікації за біометричними характеристиками;

– не вимагає від користувача ніяких додаткових дій, окрім звичних. Користувач так чи інакше, напевно, використовує пароль, який можна призначити парольною фразою, по якій проводитиметься ідентифікація/аутентифікація;

– можливість прихованої ідентифікації/аутентифікації – користувач навіть може бути не в курсі, що включена додаткова перевірка, а значить, не зможе про це повідомити зловмисника.

Але слід відзначити і недоліки даного методу:

– потребує навчання програмного засобу, що використовується для задачі ідентифікації/аутентифікації;

– сильна залежність від ергономічності клавіатури (у разі зміни, доведеться навчати програму наново);

– залежність від психофізичного стану оператора (хвороба, нервування, стан збудження і т.д.), від втомленості а також від часу доби, в який здійснюється робота користувача.

Крім того, застосування способу ідентифікації/аутентифікації по клавіатурному почерку доцільно тільки по відношенню до користувачів з досить тривалим досвідом роботи з комп'ютером і сформованою манерою роботи на клавіатурі (тобто програмісти, оператори, секретарі-референти і тому подібне). Інакше вірогідність неправильного визначення користувача істотно зростає і робить непридатним цей спосіб на практиці.

Біометрична ідентифікації/аутентифікація не визначає користувача з абсолютною точністю. З паролем все просто: він або еквівалентний еталону, або ні. Системи біометричної ідентифікації/аутентифікації пізнають користувача з певною вірогідністю, оскільки біометрична система може не упізнати легального користувача або, що ще гірше, прийняти чужого за свого. Тому усі системи біометричної ідентифікації/аутентифікації оцінюються по наступним характеристикам:

– FRR (False Reject Rate) або помилка першого роду - вірогідність помилкових відмов зареєстрованому користувачеві;

– FAR (False Accept Rate) або помилка другого роду - це вірогідність допуску незареєстрованого користувача (помилковий пропуск «чужого»);

– EER (Equal Error Rates) - рівна імовірність (норма) помилок першого і другого роду.

Ідентифікація/аутентифікація користувача по клавіатурному почерку можлива наступними способами:

– по набору ключової фрази;

– по набору довільного тексту.

Принципова відмінність цих двох способів полягає в тому, що в першому випадку використовується ключова фраза, що задається

користувачем у момент реєстрації його в системі (пароль), а в другому випадку використовуються ключові фрази, генеровані системою кожного разу у момент ідентифікації користувача.

Всі системи розпізнавання клавіатурного почерку передбачають два режими роботи: навчання і безпосередньо ідентифікація/аутентифікація.

На етапі навчання користувач вводить деяке число раз пропоновані йому тестові фрази При цьому розраховуються і запам'ятовуються еталонні характеристики цього користувача. На етапі ідентифікації/аутентифікації користувач, що претендує на доступ до комп'ютерної системи, вводить парольну фразу, для якої розраховуються характеристики клавіатурного почерку та порівнюються з еталонними.

У завданні ідентифікації користувача по клавіатурному почерку важливим етапом є обробка первинних даних. В результаті цієї обробки вхідний потік даних розділяється на ряд ознак, що характеризують ті або інші якості особи, що ідентифікується. Надалі ці ознаки піддаються статистичній обробці і дозволяють отримати ряд еталонних характеристик користувача [4, с. 237]. Найбільш зручним для практичного використання являються наступні ознаки: час утримання клавіш при наборі фрази і час між натисканням клавіш. При цьому часові інтервали між натисненням клавіш характеризують темп роботи, а час утримання клавіш — стиль роботи з клавіатурою: різкий удар або плавне натиснення. Саме аналіз цих ознак лежить в основі існуючих на сьогоднішній день підходів вивчення клавіатурного почерку [5, с. 35]. Хоча клавіатурний почерк можуть характеризувати і інші параметри: частота використання функціональних клавіш, кількість перекриттів клавіш, швидкість набору, ступінь аритмічності під час набору і т.д. Але стандартна клавіатура дозволяє виміряти тільки дві основні характеристики, зазначені вище. Проте деякі ознаки виявляються більш вагомими у визначенні індивідуальності клавіатурного почерку, тоді як інші виявляються незначними і некорисними. Слід відзначити, що оптимальний відбір ознак та характеристик клавіатурного почерку може покращити точність систем ідентифікації/аутентифікації.

Висновки. Проаналізувавши можливості комбінування звичайної парольної ідентифікації/аутентифікації користувачів з особливостями та манерою введення парольної фрази (тобто, клавіатурним почерком) можна зробити деякі висновки. По-перше, відбувається підвищення захищеності інформаційних ресурсів комп'ютерних систем за рахунок використання двох рівнів захисту. По-друге, завдяки аналізу психофізичного стану поєднання цих методів може застосовуватись в організаціях, де необхідно забезпечити високий рівень концентрації уваги співробітників під час роботи.

Основною перевагою комбінації даних методів є відсутність необхідності використання додаткового устаткування, що дозволяє створювати гнучкі підсистеми ідентифікації/аутентифікації і моніторингу дій оператора інформаційної системи, що потребує захисту. Проте, незважаючи на свої достоїнства, ця область мало вивчена, але, на мій погляд, має величезний потенціал.

Враховуючи рівень та різноманіття потенційних загроз для сучасних комп'ютерних систем можна впевнено стверджувати, що для підвищення достовірності ідентифікації/аутентифікації користувача не лише при вході в

систему, а так само в процесі роботи, необхідно використати комбінований метод, що поєднує в собі стандартні процедури введення паролів на початковому етапі і аналізу характерної поведінки зареєстрованого користувача на всьому протязі роботи в захищеній системі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ТА ЛІТЕРАТУРИ:

1. Кошева Н.А., Мазниченко Н.І. Ідентифікація користувачів інформаційно-комп'ютерних систем: аналіз і прогнозування підходів // Системи обробки інформації. Випуск 6 (113). – Харків: Харківський університет Повітряних Сил імені Івана Кожедуба, 2013. – 320 с.
2. Савинов А.Н. Методы, модели и алгоритмы распознавания клавиатурного почерка в ключевых системах: Автореф. дис. … канд. техн. наук: 05.13.19. – СПб: СПб НИУ ИТМО, 2013. – 19 с.
3. Цирлов В.Л. Основы информационной безопасности автоматизированных систем. Краткий курс: учебное пособие. – Ростов-на-Дону: Феникс, 2008. – 173 с.
4. И.А. Ходашинский, М.В. Савчук, И.В. Горбунов, Р.В. Мещеряков. Технология усиленной аутентификации пользователей информационных процессов // Управление, вычислительная техника и информатика: Доклады ТУСУРа. – 2011. – № 2(24). – Ч. 3. – С. 236-248.
5. Скуратов С. В. Использование клавиатурного почерка для аутентификации в компьютерных информационных системах // Безопасность информационных технологий — 2010. — № 2. — С. 35−38.

АКТУАЛЬНЫЕ НАУЧНЫЕ ИССЛЕДОВАНИЯ В СОВРЕМЕННОМ МИРЕ

ВЫПУСК 2(22)
Часть 1

Февраль 2017 г.

СБОРНИК НАУЧНЫХ ТРУДОВ

Выходит –12 раз в год (ежемесячно)
Издается с июня 2015 года

Включен в наукометрические базы:

РИНЦ http://elibrary.ru/title_about.asp?id=58411
Google Scholar
https://scholar.google.com.ua/citations?user=JP57y1kAAAAJ&hl=uk
Бібліометрика української науки
http://nbuviap.gov.ua/bpnu/index.php?page_sites=journals
Index Copernicus
http://journals.indexcopernicus.com/++++,p24785301,3.html

Переяслав-Хмельницкий

УДК 001.891(100) «20»
ББК 72.4
А43

Актуальные научные исследования в современном мире: XXII Междунар. научн. конф., 26-27 февраля 2017 г., Переяслав-Хмельницкий. // Сб. научных трудов - Переяслав-Хмельницкий, 2017. - Вып. 2(22), ч. 1 – 154 с.

Языки издания: українська, русский, english, polski, беларуская, қазақша, o'zbek, limba română, кыргыз тили, Հայերեն

В сборнике представлены результаты актуальных научных исследований ученых, докторантов, преподавателей, аспирантов и студентов - участников Международной научной конференции **"Актуальные научные исследования в современном мире"** (Переяслав-Хмельницкий, 26-27 февраля 2017 г.).

Сборник предназначен для научных работников и преподавателей высших учебных заведений. Может использоваться в учебном процессе, в том числе в процессе обучения аспирантов, подготовки магистров и бакалавров в целях углубленного рассмотрения соответствующих проблем. Все статьи сборника прошли рецензирование, сохраняют авторскую редакцию, всю ответственность за содержание несут авторы.

УДК 001.891(100) «20»
ББК 72.4
А43