УДК 004.056.5

В.М. Білоус
К.Р. Дзюбенко

СИСТЕМА БЕЗПЕРЕРВНОЇ АВТЕНТИФІКАЦІЇ НА ОСНОВІ ФОНОВОГО АНАЛІЗУ ПОВЕДІНКОВОЇ БІОМЕТРІЇ

Вінницький національний технічний університет

Анотація

У роботі розглядається проблема забезпечення надійного захисту інформаційних систем від несанкціонованого доступу та перехоплення сеансів. Запропоновано вдосконалений метод безперервної автентифікації користувачів, який базується на комплексному аналізі поведінкових біометричних характеристик: динаміки клавіатурного почерку та патернів руху мишкою. Метод передбачає використання алгоритмів машинного навчання для одночасної обробки обох типів даних та формування унікального поведінкового профілю у фоновому режимі. Реалізація запропонованого підходу дозволить підвищити точність ідентифікації легітимного користувача, знизити рівень хибних спрацьовувань та забезпечити непомітну перевірку протягом усього сеансу роботи.

Ключові слова: безперервна автентифікація, поведінкова біометрія, клавіатурний почерк, патерни руху мишкою, інформаційна безпека, машинне навчання, поведінковий профіль.

Abstract

The paper addresses the problem of ensuring reliable protection of information systems against unauthorized access and session hijacking. An improved method for continuous user authentication based on the comprehensive analysis of behavioral biometric characteristics specifically keystroke dynamics and mouse movement patterns is proposed. The method involves using machine learning algorithms for the simultaneous processing of both data types and the generation of a unique behavioral profile in the background. The implementation of the proposed approach will improve the accuracy of legitimate user identification, reduce the false acceptance rate, and provide imperceptible verification throughout the entire session.

Keywords: continuous authentication, behavioral biometrics, keystroke dynamics, mouse movement patterns, information security, machine learning, behavioral profile.

Вступ

В умовах стрімкого розвитку інформаційних технологій та поширення віддаленого доступу проблема захисту систем від несанкціонованого втручання набуває особливої актуальності. Після успішної первинної авторизації активна сесія залишається вразливою до перехоплення або використання сторонніми особами у разі залишення робочого місця без нагляду, що суттєво знижує загальний рівень безпеки інформаційної системи.

Одним із перспективних підходів до розв'язання зазначеної проблеми є застосування технологій безперервної автентифікації, що передбачають фоновий моніторинг поведінкової біометрії користувача, зокрема динаміки клавіатурного почерку та патернів руху мишкою. Особливої уваги потребує вдосконалення методів комплексного аналізу цих показників із використанням машинного навчання, що дозволить підвищити точність розпізнавання та мінімізувати кількість хибних блокувань.

Незважаючи на перспективність цього напряму, більшість існуючих рішень базуються на аналізі лише однієї модальності або використовують жорсткі алгоритми, які не здатні гнучко адаптуватися до природних змін у поведінці людини, що робить розроблення більш інтелектуальних систем актуальним завданням.

Результати дослідження

Традиційні системи захисту інформації стикаються з проблемою перехоплення сеансів, оскільки після первинної автентифікації система більше не перевіряє особу користувача. У зв'язку з цим значна увага в сучасних дослідженнях приділяється поведінковій біометрії, зокрема аналізу клавіатурного почерку та динаміки миші, які дозволяють безперервно автентифікувати користувача без використання додаткового апаратного забезпечення [1].

Для реалізації алгоритмів безперервної автентифікації найчастіше аналізують окремі модальності. Механізми оцінки клавіатурного почерку фокусуються на часових затримках, тоді як динаміка миші враховує швидкість переміщення, координати та частоту кліків. Проте використання лише одного пристрою введення може бути менш стійким до хибних спрацьовувань, тому сучасний підхід полягає в об'єднанні цих двох джерел даних для створення комплексного поведінкового профілю [2].

Важливим напрямом є розробка інтелектуальних програмних інструментів, що використовують передові методи машинного навчання для глибокого аналізу зібраної біометрії. На відміну від класичних систем захисту, які спираються на жорсткі правила або статичні порогові значення, моделі машинного навчання здатні виявляти приховані, нелінійні закономірності у діях людини. Оскільки поведінка користувача не є абсолютно стабільною і може залежати від зовнішніх факторів, психоемоційного стану або втоми, інтелектуальні алгоритми дозволяють відфільтровувати такий «шум» і зосереджуватись на справді унікальних ідентифікаційних ознаках [3].

Дана робота пропонує покращення існуючих механізмів безперервної автентифікації за рахунок впровадження ансамблевих алгоритмів машинного навчання. Це вдосконалення дозволяє ефективно обробляти мультимодальні дані та динамічно адаптуватися до природних змін у поведінці користувача. Суть таких алгоритмів полягає в об'єднанні результатів роботи кількох незалежних класифікаторів у єдине рішення, що значно знижує ймовірність помилки та підвищує стійкість системи до спроб імітації легітимного користувача зловмисником. Для практичної реалізації системи передбачається розробка спеціалізованого програмного забезпечення, що дозволить створити оптимізовану фонову службу на рівні операційної системи для непомітного перехоплення подій вводу без переривання робочого процесу [4].

Практична реалізація запропонованого методу базується на послідовному алгоритмі обробки інформації. На першому етапі фонова служба здійснює безперервне перехоплення подій введення: фіксуються часові затримки клавіатурного вводу, швидкість переміщення та кліки миші. Спочатку зібрані дані використовуються для первинного навчання моделі у режимі пасивного моніторингу, що дозволяє непомітно сформувати еталонний поведінковий профіль на основі типових повсякденних дій легітимного користувача. На другому етапі, вже під час активного захисту сеансу, ці дані перетворюються у вектори ознак і передаються до модуля машинного навчання, який порівнює поточну поведінку з раніше створеним еталонним профілем користувача. На фінальному етапі ансамблевий алгоритм динамічно обчислює «рівень довіри» до активної сесії. Якщо цей показник падає нижче критичного порогу, система генерує сигнал тривоги та автоматично блокує робочий екран, унеможливлюючи подальший несанкціонований доступ.

Для кількісної оцінки ефективності таких систем найчастіше використовуються метрики рівня хибного допуску (FAR) та рівня хибної відмови (FRR). Застосування ансамблевого машинного навчання до комбінованих даних клавіатури та миші дозволяє суттєво знизити ці показники, забезпечуючи точність розпізнавання легітимного користувача понад 95% у реальному часі [5].

Таким чином, запропонований метод, що об'єднує безперервний моніторинг клавіатури та миші з ансамблевими алгоритмами машинного навчання, дозволяє сформувати максимально точний поведінковий профіль. Практичне створення такої системи забезпечить розпізнавання легітимного користувача в режимі реального часу, зводячи до мінімуму рівень хибних спрацьовувань та гарантуючи миттєве блокування несанкціонованого доступу.

Висновки

У роботі запропоновано вдосконалений метод безперервної автентифікації користувачів інформаційних систем із використанням комплексного аналізу поведінкової біометрії, яка передбачає фоновий збір показників клавіатурного почерку та динаміки миші з подальшим застосуванням інтелектуальних алгоритмів для їх обробки. Це дозволяє динамічно оновлювати еталонний профіль користувача та ефективно відрізняти його легітимні дії від спроб імітації чи перехоплення управління.

Обгрунтовано доцільність розроблення спеціалізованого програмного забезпечення, яке забезпечує надійний захист активних сеансів від несанкціонованого доступу, сприяє підвищенню загального рівня інформаційної безпеки, а також може бути використане в корпоративних мережах для автоматичного виявлення аномалій та миттєвого блокування скомпрометованих робочих місць.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. User Authentication Method Based on Keystroke Dynamics and Mouse Dynamics with Scene-Irrelated Features in Hybrid Scenes. MDPI, 2022. DOI: https://doi.org/10.3390/s22176627

2. Continuous Authentication Based on Keystroke and Mouse Dynamics in Video Private Network. IEEE Xplore, 2022. DOI: https://doi.org/10.1109/ICICN52636.2021.9673832

3.Wrist in Motion: A Seamless Context-Aware Continuous Authentication Framework Using Your Clickings and Typings. IEEE Xplore, 2020. DOI: https://doi.org/10.1109/TBIOM.2020.2997004

4. Deep Learning-Driven User Legitimacy Prediction Using Keystroke and Mouse Behavioural Dynamics. IEEE Xplore, 2025. DOI: https://doi.org/10.1109/ICCA62237.2024.10928042

5. Behaviour Biometrics Using AI for Continuous Authentication Systems. ResearchGate, 2025. DOI: https://doi.org/10.60087/jaigs.v8i02.386

Дзюбенко Костянтин Романович – студент групи 1КІТС-22б, Факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: roman06.04.2016@gmail.com

Науковий керівник: Білоус Віталій Михайлович – асистент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця, e-mail: pydev@ukr.net

Dziubenko Kostiantyn R. – student of group 1KITS-22b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: roman06.04.2016@gmail.com

Supervisor: Bilous Vitaliy M – assistant professor of the Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: pydev@ukr.net