DOI 10.36074/logos-31.03.2023.29

ДОСЛІДЖЕННЯ МЕТОДІВ ТА МОДЕЛЕЙ АВТЕНТИФІКАЦІЇ НА ОСНОВІ ДАНИХ ПРО ВЗАЄМОДІЮ З КЛАВІАТУРОЮ

Кайдалов Вадим Дмитрович
Здобувач вищої освіти факультету комп'ютерних наук
Харківський національний університет радіоелектроніки

НАУКОВИЙ КЕРІВНИК:

ORCID ID: 0000-0001-5981-4760 **Віра Володимирівна Голян**
канд. техн. наук, доцент, доцент кафедри програмної інженерії
Харківський національний університет радіоелектроніки

УКРАЇНА

Активні та пасивні методи автентифікації – це два різних способи перевірки ідентичності особи. Активні методи автентифікації вимагають, щоб користувач активно надавав інформацію або виконував дії для підтвердження своєї ідентичності. Це може включати такі методи, як введення пароля або PIN-коду, надання скану відбитку пальця чи склери ока, або відповіді на питання з безпеки. Пасивні методи автентифікації, з іншого боку, не вимагають від користувача активних дій або дії з його сторони. Ці методи, як правило, полягають у моніторингу поведінки або фізичних характеристик користувача для перевірки його ідентичності. Наприклад, система може використовувати такі біометричні дані, як розпізнавання обличчя або ритм набору тексту, щоб безперервно перевіряти ідентичність користувача під час використання пристрою або програми. Пасивні методи автентифікації часто використовуються в ситуаціях, де зручність є пріоритетом, наприклад, для розблокування смартфона або доступу до часто використовуваної програми. Основна різниця між активними та пасивними методами автентифікації полягає у рівні взаємодії користувача. Активна автентифікація вимагає від користувача вжиття дій, тоді як пасивна автентифікація працює в фоновому режимі, без необхідності в конкретних діях з боку користувача. Обидва методи мають свої переваги та недоліки, і вибір відповідного методу залежить від конкретної ситуації використання та вимог щодо безпеки.

Автентифікація за ритмом набору тексту є типом пасивної автентифікації, яка працює в фоновому режимі без необхідності в конкретних діях з боку користувача. Вона передбачає аналізування способу набору тексту користувачем, включаючи його швидкість набору, тривалість натискання клавіш, час між натисканнями та інші особливості поведінки набору тексту. Ці характеристики є унікальними для кожної людини і можуть бути використані для створення профілю набору тексту, який можна використовувати для автентифікації [1].

Для використання автентифікації за ритмом набору тексту користувач зазвичай набирає зразок тексту або вводить кодову фразу, а система аналізує його характеристики набору тексту для створення профілю. Після цього, коли користувач наступного разу входить у систему, система порівнює його характеристики набору тексту зі збереженим профілем для визначення

співпадіння. Якщо характеристики набору тексту співпадають, користувачу надається доступ; якщо ні – у доступі відмовляється.

Автентифікація на основі динаміки натискання клавіш полягає у захопленні часу затримки між натисканням клавіш, часу, необхідного для їх відпускання, та інтервалів між натисканнями клавіш для створення унікального біометричного профілю для кожного користувача. Ці методи аналізують, як користувачі набирають текст та ритм їх письма і використовують ці дані, щоб ідентифікувати користувача.

Існують два основних підходи до автентифікації на основі динаміки натискання клавіш: статичний і динамічний. Статична автентифікація на основі динаміки натискання клавіш використовує лише одноразовий процес реєстрації, щоб створити профіль ритму набору тексту користувача. Цей метод менш точний, оскільки не враховує змін у ритмі письма користувача з плином часу.

Динамічна автентифікація на основі динаміки натискання клавіш постійно відслідковує та оновлює профіль ритму набору тексту користувача з плином часу. Вона використовує алгоритми машинного навчання для адаптації до змін у поведінці користувача, покращуючи точність та зменшуючи кількість помилкових результатів.

Таким чином, автентифікація на основі динаміки натискання клавіш може забезпечити високий рівень безпеки при цьому не заважаючи користувачу, але вона може бути вразливою до помилкових позитивів, якщо користувач перебуває під стресом або набирає текст у середовищі, яке відрізняється від звичайного.

Модель машинного навчання для автентифікації на основі динаміки натискання клавіш можна побудувати, використовуючи алгоритми навчання з учителем, такі, як класифікатор на основі методу опорних векторів (SVM), нейронні мережі або різні комбінації цих методів [2]. Спочатку модель навчається на певній кількості даних, зібраних від користувачів. Ці дані включають інформацію про час затримки між натисканням та відпусканням клавіш, а також про час затримки між натисканням різних клавіш. Після навчання модель може використовуватися для автентифікації користувача в режимі реального часу, порівнюючи його динаміку натискання клавіш зі зразками даних, вивченими на етапі навчання.

Загалом, модель на основі динаміки натискання клавіш може забезпечити високий рівень безпеки, не заважаючи користувачу, але може бути вразлива до помилкових позитивів, якщо користувач перебуває у стресовій ситуації або набирає текст в іншому середовищі, ніж зазвичай.

Список використаних джерел:

[1] Teh, Pin Shen & Teoh, Andrew & Yue, Shigang (2013). A Survey of Keystroke Dynamics Biometrics. The Scientific World Journal, (2013). https://doi.org/10.1155/2013/408280.

[2] Zhong, Yu & Deng, Yunbin (2015). A Survey on Keystroke Dynamics Biometrics: Approaches, Advances, and Evaluations. GCSR, (2), 1-22. https://doi.org/10.15579/gcsr.vol2.ch1.