Артамонов Є.Б., к.т.н., доцент,
Крант Д.В., аспірант,
Національний авіаційний університет

МЕТОД ДОДАТКОВОЇ АУТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ ЧЕРЕЗ АНАЛІЗ ПОВЕДІНКОВИХ ОЗНАК КОРИСТУВАЧА

При роботі з онлайновими системами є небезпека втрати викрадення паролів у користувачів. Тому організації можуть зменшити ризик викрадення паролів та несанкціонованого доступу до внутрішніх баз даних, встановлюючи додаткові заходи безпеки, наприклад:

– вимагати складні паролі та періодичну зміну паролів.

– забезпечити шифрування даних на рівні бази даних та взаємодії з нею.

– встановлювати доступ до внутрішніх баз даних лише для обмеженої групи користувачів, що мають певні дозволи та права.

– перевіряти активність користувачів та відслідковувати незвичайну активність.

– використовувати додаткові методи аутентифікації, такі як біометричні дані.

– забезпечити регулярне оновлення програмного забезпечення та встановлення патчів безпеки.

– проводити навчання користувачів щодо забезпечення безпеки та правил обробки конфіденційної інформації.

Для реалізації методу аналізу поведінкових ознак користувача для додаткової аутентифікації користувачів можна ввести оцінку відношення стилю роботи користувача і порівняння цієї оцінки з збереженою в системі:

$$d = \sqrt{\omega_1 \left(x_1 - y_1\right)^2 + \omega_2 \left(x_2 - y_2\right)^2 + ... + \omega_n \left(x_n - y_n\right)^2},$$

де d – це відстань між оцінкою поведінки користувача і його збереженою оцінкою поведінки,

$x_1, x_2, ..., x_n$ – значення параметрів користувача, який перевіряється,

$y_1, y_2, ..., y_n$ – значення збережених параметрів,

$\omega_1, \omega_2, ..., \omega_n$ –вагові коефіцієнти.

За практичним дослідженням було виявлено коливання різниці оцінок, тому за рахунок коригування розміру всіх вагових коефіцієнтів коливання було обмежене діапазоном [0; 0,1].

В разі виходу оцінки за межі діапазону в першу чергу перевіряється чи не було входу в систему одного з зареєстрованих користувачів. Для цього знаходимо користувача з мінімальною оцінкою різниці:

$min\ \{di\}$,

$$d_i = \sqrt{\omega_1 \left(x_1 - y_{1i}\right)^2 + \omega_2 \left(x_2 - y_{2i}\right)^2 + ... + \omega_n \left(x_n - y_{ni}\right)^2},$$

де d_i – це відстань між оцінкою поведінки користувача, що аналізується, і збереженою оцінкою поведінки i-го користувача,

$x_1, x_2, ..., x_n$ –значення параметрів, що перевіряються,

$y_{1i}, y_{2i}, ..., y_{ni}$ –значення збережених параметрів i-го користувача,

$\omega_1, \omega_2, ..., \omega_n$ –вагові коефіцієнти.

Для розрахунку $y_1, y_2, ..., y_n$ можуть бути використані значення, отримані зі збору даних користувачів на підставі цих параметрів. Наприклад, якщо для користувача 1 були зібрані наступні значення:

– кількість натискань на клавішу за 5 секунд: 15;

– кількість помилок при наборі тексту на 10 символів: 2;

– кількість переглядів каталогів за хвилину: 3;

– кількість кліків миші за 10 секунд: 5.

Тоді значення у для кожного параметра можуть бути обчислені наступним чином:

– y_{11}= 15;

– y_{21} = 2;

– y_{31} = 3;

– y_{41} = 5.

Важливо зазначити, що вибір та обчислення поведінкових параметрів залежить від конкретної задачі, а також від технічних можливостей збору та аналізу поведінкових даних.

Висновки

Методи аналізу поведінкових ознак користувачів дозволяють визначити унікальний шаблон поведінки кожного користувача і використовувати його для аутентифікації. Це знижує ризик роботи з системою викрадача паролю, оскільки змінити поведінкові параметри важко.

Проте, важливо враховувати ризики та обмеження методів поведінкової біометрії. Користувач може змінити свій шаблон поведінки, наприклад, змінити стиль набору тексту або швидкість набору, що може спричинити помилки в аутентифікації. Для досягнення максимальної ефективності, методи поведінкової аутентифікації можуть бути поєднані з іншими методами аутентифікації, такими як двофакторна аутентифікація або використання сильних паролів. Комбінування декількох методів аутентифікації може допомогти зменшити ризики та підвищити безпеку користувача.

Застосування методів поведінкової біометрії в бізнес-середовищах може бути складним, оскільки вони вимагають спеціального програмного забезпечення та обладнання, що може збільшити витрати на забезпечення безпеки.