УДК 004.031.6
О. Багрій
(Тернопільський національний технічний університет імені Івана Пулюя)

АНАЛІЗ ЗАСОБІВ АУТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ НА ОСНОВІ КЛАВАТУРНОГО ПОЧЕРКУ

UDC 004.031.6
O. Bagriy

ANALYSIS OF KEYBOARD-BASED USER AUTHENTICATION MEANS

На сьогоднішній день кількість рішень щодо аутентифікації користувачів на основі динаміки їхньої роботи з клавіатурою персонального комп'ютера постійно збільшується. І якщо раніше дані системи обмежувалися лише аналізом введення пари логін/пароль (розглядалася виключно статична аутентифікація), то зараз активно розвиваються системи,здатні аналізувати поведінку користувача за комп'ютером безперервно.

BehavioWeb (рисунок 1). Одним з найбільш відомих комерційних рішень у галузі безперервної фонової аутентифікації користувачів за клавіатурним почерком є продукт BehavioWeb компанії BehavioSec. Для аналізу поведінки користувача у ньому використовуються ритм та швидкість набору тексту, а також сила натискання на клавіші.

Програмне забезпечення вбудовується у веб-сайт або додаток. Для цього використовуються JavaScript-бібліотека, що поставляється, а також J2EE-модуль, що вбудовується bweb-сервер для здійснення процедури автентифікації. Розробники звертають увагу на те, що їхнє рішення аналізує зміну характеристик введення користувача з часом і періодично оновлює модель користувача. Проте,алгоритми, що використовуються для цього, не називаються.

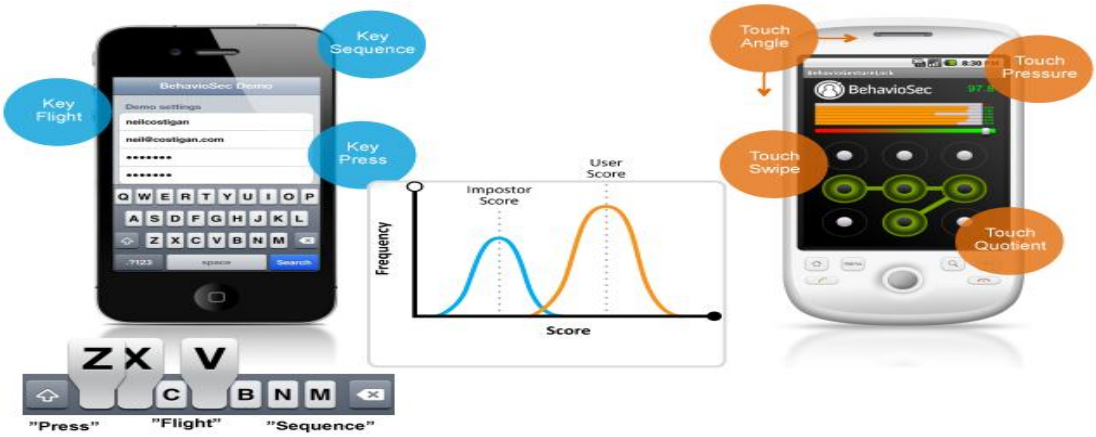

Рисунок 1. Система BehavioWeb

KeyTrac (рисунок 2). Не менш популярним рішенням є продукт KeyTrac [4, 5],що дозволяє здійснювати у фоновому режимі як автентифікацію, так ідентифікацію користувачів комп'ютера, ґрунтуючись на динаміці їх клавіатурного введення. Дані користувачів (тривалість натискання на клавіші клавіатури, а також тривалості перескоку між клавішами) записуються за допомогою компонента KeyTrac Recorder і відправляються на сервер компанії, де відбувається їх порівняння із побудованою раніше моделлю. При цьому побудова моделі користувача здатна здійснюватися на будь-якому довільному тексті, а не тільки при багаторазовому введенні тих самих фраз. Для передачі даних використовується наданий KeyTrac API. Далі сервер повертає свій вердикт у вигляді булевоївеличини true/false – чи

відповідають надіслані тестові дані розглянутому легітимного профілю чи ні. Для вбудовування цього рішення на веб-сайт також пропонується використовувати JavaScript-бібліотеку, що надається. Розробники системи стверджують, що їх рішення нечутливе до зміни мови, що використовується, а також до зміни обладнання, що використовується. Використовувані для цього алгоритми, а також методи побудови моделі та їх подальшої класифікації не називаються.

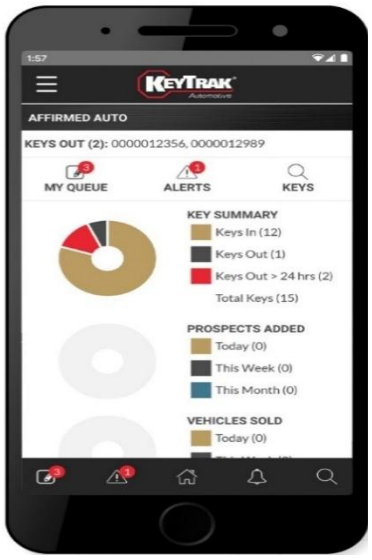

Рисунок 2. Система KeyTrac

Література

1. Peltier, T. R. Information security risk analysis, Third Edition. CRC Press, 2020. 456 p.
2. Olsson, T. Assessing security risk to a network using a statistical model ofattacker community competence. Proceedings of the 11th internationalconference on Information and Communications Security. 2019. P. 308–324.
3. Peltier, T. R. Information security risk analysis, Third Edition. CRC Press, 2020. 456 p