УДК 004.056.523

ДОСЛІДЖЕННЯ ІНФОРМАТИВНИХ ОЗНАК СЕНСОРНОГО ПОЧЕРКУ ВЛАСНИКІВ МОБІЛЬНИХ ПРИСТРОЇВ

Омельченко А.Л.
Науковий керівник – к.т.н., доц. Горелов Д.Ю.
Харківський національний університет радіоелектроніки,
студентський науковий гурток «Біометричні технології контролю доступу»
каф. КРіСТЗІ, м. Харків, Україна
тел. +38(057) 702-14-30, e-mail: alina.omelchenko@nure.ua

In the study the informative features of mobile keystroke dynamics are analyzed. The Multi-Class Classification accuracy by the Random forest method of users from the "The Mobikey Keystroke Dynamics Password Database" by time and psycho-physiological parameters is 94.7%. The Binary Classification accuracy is not less than 90%. FAR is 1.58 %. FRR is 1.36 %.

Класичні методи ідентифікації (відбиток пальця, 2D та 3D геометрія обличчя) вже стали звичними – і майже настільки ж звичною стала інформація про те, як зловмисники можуть зламувати ці технології. Альтернативою цим методам є так званий «відбиток мобільного пристрою». У цьому випадку використовують такі характеристики, як модель пристрою, операційна система, додатки, що використовує користувач, параметри Wi-Fi-мереж, до яких часто підключається користувач, технічні параметри пристроїв, що користувач підключає до смартфону. В результаті система створює свого роду профіль і пристрою, і звичок конкретного користувача. Якщо система виявляє нетиповий сценарій використання мобільного пристрою, вона використовує додаткові способи перевірки (паролі, контрольні питання тощо).

Однак цьому методу ідентифікації заважає те, що і Apple, і Google обмежують набір параметрів, які можна отримати про пристрій віддалено. Це робиться з метою захисту особистих даних користувачів. Тому розвиваються нові методи біометричної ідентифікації. В першу чергу це так звана поведінкова біометрія. В її основі лежить цілий ряд параметрів, що характеризують поведінку конкретного користувача. Так, наприклад, використовувані в смартфоні гіроскопи і акселерометри можуть оцінити і запам'ятати, як людина тримає смартфон під час використання, в якому становищі зазвичай носить його і навіть як ходить. За допомогою тачскріну і клавіатури можна встановити характерні для людини рухи рук і пальців.

У роботі проаналізовано інформативні ознаки сенсорного почерку. Можна виділити три основних класи: часові параметри, параметри взаємодії з екраном (тиск та розмір «плями» від пальця) та психофізіологічні параметри, де до тиску та розміру «плями» додаються показання акселерометру та динаміка руху кінчика пальця по екрану.

За даними датасету «The Mobikey Keystroke Dynamics Password Database» інтегральна точність мультикласової класифікації за сенсорним почерком становить 94.7 %. Отже, системи розпізнавання за сенсорним почерком можуть забезпечити точність ідентифікації, яка притаманна системам ідентифікації за клавіатурним почерком. Проте для забезпечення такої точності необхідно збирати більші масиви даних: пароль «.tie5Roanl» в дата сеті «MOBIKEY strong» (для сенсорного почерку) містить 72 інформативних параметри, в той час як пароль «.tie5Roanl» в дата сеті «Keystroke Dynamics Benchmark Data Set» (для клавіатурного почерку) містить 31 інформативний параметр.

Точність розпізнавання за часовими параметрами сенсорного почерку становить 83 %. Таким чином, нестабільність часових параметрів сенсорного почерку обумовлює неможливість побудови систем ідентифікації, що враховують лише ці часові параметри.

Точність розпізнавання за параметрами взаємодії з екраном складає 67.7 %. Таким чином, тиск та розмір «плями» не є унікальними параметрами сенсорного почерку.

Найінформативнішими параметрами сенсорного почерку є прискорення по трьох осях координат, динаміка руху кінчика пальця по екрану та усереднений час натискання клавіш в процесі набору парольної фрази. Використання цих семи параметрів дає інтегральну точність мультикласової класифікації 91.1 %.

Підвищити точність ідентифікації можна за рахунок побудови двійкової системи класифікації, коли цільовому користувачу присвоюється клас 1, тобто «зареєстрований», а усім іншим користувачам – клас 2, тобто «зловмисник». Це можливо, оскільки на відміну від комп’ютера, де зареєстрованими користувачами можуть бути декілька людей, у мобільного пристрою завжди тільки один власник.

Проведені дослідження дозволяють зробити висновок про забезпечення інтегральної помилки FAR 1.58 %. Враховуючи також той факт, що зловмисник апріорі має сформований сенсорний почерк, оскільки сфера його професійних навичок вимагає тривалого часу взаємодії зі смартфонами (один з пари користувачів вже має унікальний почерк), то з плином часу значення помилки FAR буде зменшуватись, оскільки інформативні ознаки сенсорного почерку легітимного користувача також ставатимуть більш унікальними (обидва користувачі в парі мають унікальний почерк). За результатами проведених досліджень можна очікувати зменшення рівня помилки FAR до 1.2 %, тобто 12 пропусків зловмисника на 1000 спроб.

Рівень помилки FRR (доступ заборонений користувачеві, зареєстрованому в системі) за умови недосвідченого користувача може становити до 1.36 %. Якщо ж враховувати лише користувачів з унікальним почерком, то рівень помилки FRR зменшується до 0.54 %, тобто 54 недопуски верифікованого користувача на 10000 спроб.