

ИСПОЛЬЗОВАНИЕ ИДЕНТИФИКАЦИИ ПО КЛАВИАТУРНОМУ ПОЧЕРКУ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

USE OF IDENTIFICATION BY KEYBOARDING IN INFORMATION SECURITY

B. Shvyrev

Summary. The article gives an overview of scientific research devoted to the study of user identification by such a biometric unique characteristic as a keyboard highlight. Abstract describes methods of mathematical and statistical data processing that are used by the researchers when typing on the keyboard, as well as the results obtained. The features of the keyboard highlight and means of its registration are given.

Keywords: keyboard handwriting, user authentication, mathematical models, the interval between clicks, the duration of pressure.

Швырев Борис Анатольевич

К.ф.-м.н., в.н.с., Научно-исследовательский институт
ФСИН России, г. Москва, Россия
bor2275@yandex.ru

Аннотация. В статье приводится обзор научных исследований, посвященных изучению идентификации пользователей по такой биометрической уникальной характеристике как клавиатурный почерк. Реферативно описываются используемые исследователями приемы математической и статистической обработки данных формируемых при наборе текста на клавиатуре, а также полученные результаты. Приведены особенности клавиатурного почерка и средств его регистрации.

Ключевые слова: клавиатурный почерк, аутентификация пользователей, математические модели, интервал между нажатиями, длительность нажатия.

Уникальность клавиатурного почерка доказывает множество проводимых экспериментов. Одним из очевидных фактов наличие индивидуальных особенностей у радистов, использующих азбуку Морзе (или работающих на ключе). Во время войны радисты узнавали друг друга в эфире по особенностям передачи длительности пауз, темпу ввода точек, интенсивности всей передачи и т.д.

Идентификация по клавиатурному почерку аналогична распознаванию рукописного почерка, но в место анализа наклона и прочих характеристик, приведенных в работе [1] таких как сила движения, динамичность, напряженность, содержательность; вытянутость букв; степень связанности букв в слове и т.д., анализу подвергаются временные характеристики набора символов на клавиатуре: время нажатия, время удержания клавиш.

Первое предложение использовать динамику нажатия клавиши для аутентификации пользователей появилось в 1974 [2]. С тех пор исследователи разработали системы аутентификации пользователей по динамике нажатия клавиши, используя различные методы [3] распознавания образов как нейронные сети [4–7], статистические методы классификации [8–11], деревья решений [12], моделирование на основе скрытых Марковских процессов [13–15]. Ряд работ посвящено использованию аппарата нейронных сетей [16–18].

В [19] идентификация пользователя осуществлялась по имени пользователя, при этом дополнительного па-

роля не использовалось. Эталонные значения формировались по паузам между нажатиями по последним 30 вводам имени. Решение принималось по двум методам: минимального расстояния и классификатора Байеса. Идентификация пользователя отклонялась, когда по каждому критерию порог выбора решения не был превышен.

Для идентификации пользователей авторы в работе [20] рассматривали оба интервала при наборе текста. Регистрировались интервалы между нажатиями и продолжительность удержания клавиши при наборе текста. Для определения пользователя лучшие результаты были получены по времени удержания клавиши. В работе отмечено значительное улучшение идентификации при использовании расчетов по обоим типам измерений. По результатам тестов авторы признали лучшими следующие методы:

- ◆ нейронные методы: нечеткий ARTMAP (обобщенная теория адаптивного резонанса сети ART с операциями теории нечетких множеств), RBFN (радиально базисные функции сети), LVQ (Обучаемая векторная квантизация);
- ◆ статистические методы с учетом потенциальной диаграммы и критерия Байеса.

В статье S.J. Shepher [21] исследовал непрерывную аутентификацию для расчета необходимого наименьшего количества нажатий для быстрого определения пользователя с достаточной вероятностью. Автор рассматривал особенности аутентификации на коротких тестах, и обнаружил, что 100 символов достаточно для иденти-

фикации пользователя. Для идентификации использовались средние значения и дисперсия интервалов между нажатиями и длительность надавливания.

В исследованиях [22–24] отмечается, что время удержания клавиши более эффективно для аутентификации пользователя, чем время задержки нажатия и отпускания и интервал между нажатием и отпусканием предыдущей клавиши. Время удержания конкретной клавиши (символа) одним пользователем является случайной величиной. Плотность вероятности этой величины полагают подобной Гауссовскому распределению плотности вероятности [25–28]. На основе таких предположений используется скрытая модель Марковского процесса для описания динамики нажатия на клавиши [15]. В [15] измерения времени удержания осуществляется с интервалом порядка более 20 мс.

В [29] измеряли временные интервалы между нажатиями клавиш при вводе полного имени и пароля, для регистрации нового пользователя требовалось повторить ввод восемь раз. По измеренным значениям рассчитывались средние значения и дисперсия для каждого слова. По рассчитанным значениям определялись пороговые значения, с которыми сравнивались текущие для принятия решения.

А. Ю. Комиссаров и А. В. Подлесный [30] выполняли аутентификацию пользователей по значениям параметров клавиатурного почерка времени удержания каждой из клавиш и паузы между нажатиями соседних клавиш, при наборе одной и той же для всех пользователей ключевой фразы.

Проведенный анализ научных работ показал большой интерес ученых разных стран к проблеме исследования идентификации пользователя по клавиатурному почерку.

Существующие на рынке системы идентификации пользователей по клавиатурному почерку пока не обеспечивают высокой достоверности, что не позволяет их использовать самостоятельным методом. Увеличение надежности идентификации пользователя наблюдается при совместном использовании ключевого слова и аутентификации по клавиатурному почерку.

Американская компания BioNetSystem разработала и запатентовала систему аутентификации пользователя по динамике клавиш BioPassword [31–33], называемую в литературе так же клавиатурным почерком. Система интегрируется в сетевые компьютеры для разграничения доступа. Идентификация пользователя осуществляется по биометрическому шаблону. Который формируется путем ввода с клавиатуры имени и пароля несколько раз подряд минимум 15 раз.

Система тестировалась на сервере Windows и рабочих станциях [34], во время проверки формировались удовлетворительные результаты.

Особенности сетевой идентификации по клавиатурному почерку рассматривались в [35, 36]. Передача регистрационной информации: имя и пароля в сети осуществляются IP-пакетами, которые формируются с интервалом кратным 50 мс. В исследовании полагали распределение интервалов между нажатиями клавиш подобным Гауссовскому, и для описания использовали математическое ожидание и дисперсию. Решение о приеме учетных данных осуществлялось по попаданию измеренных значений в интервал допустимых для конкретного пользователя. Интервал составлял порядка 50 мс. Для правильной идентификации пользователь должен обладать сильным различием в скорости набора текста на компьютере. Существуют так же продукты компании iMagic Software и Deep Net Technologies позволяющие идентифицировать пользователя по динамике набора. В настоящее время все имеющиеся коммерческие решения обеспечивают не высокую достоверность, что не позволяет их использовать как самостоятельную систему. Целесообразно их использовать совместно с проверкой имени и пароля.

В рассмотренных работах анализировались экспериментальные данные пользователей, обладающих навыком скоростного набора текста или десятипальцевым методом, называемым, также слепым методом набора. Наличие особенности набора текста у таких пользователей очевиден, что позволяет отличать их на разных тестах. Как показывает практика, при длительном наблюдении каждый пользователь имеет свои индивидуальные особенности. Для их регистрации необходимо использовать более чувствительные методы анализа. Помимо методов анализа слабых, не очевидных зависимостей необходимо использовать измерительные средства с большей точностью, сюда относится точность измерения временных характеристик событий клавиатуры. Исходя из особенности работы и функционирования самого медленного устройства вычислительной техники — клавиатуры необходимо повышение точности регистрации временных событий. В рассмотренных работах описание индивидуальных особенностей осуществляли по интервалу времени между нажатиями клавиш и значениями времени удержания нажатой клавиши. Отмечается продолжительное время шага, с которым регистрируются эти события. Шаг регистрации составляет порядка от полутора до трех — пяти десятков миллисекунд. Таким образом, целесообразно исследовать особенности формирования и регистрации событий клавиатуры для уточнения выбранных предварительных математических моделей клавиатурного почерка.

Проведенный обзор существующих результатов показал растущий интерес к использованию идентификации пользователей по клавиатурному почерку. Этот метод пока не обеспечивает высоких вероятностных показателей идентификации, но обладает рядом несомненных преимуществ, это недорогой инструмент идентификации, имеющийся у любой вычислительной

техники, высокая скрытность представления и защита от копирования и подделки, а также использование только дополнительного программного обеспечения, что легко интегрируется в операционную систему. Для широкого внедрения этого метода необходимы более адекватные модели процесса набора текста на клавиатуре.

ЛИТЕРАТУРА

1. Зуев-Инсаров Д. М. Строение почерка. [Электронный ресурс]. — URL: <http://www.biblionline.ru/goods.php?id=460> (дата обращения: 09.02.2018)
2. R. Spillane, «Keyboard Apparatus for Personal Identification», IBM Technical Disclosure Bulletin, vol. 17, 1975.
3. Jarmo Ilonen Keystroke dynamics. Lappeenranta University of Technology, Skinnarilankatu 34, 53850 Lappeenranta, Finland.
4. D. Bleha and Obaidat, M. Dimensionality reduction and feature extraction applications in identifying computer users. IEEE Transactions on Systems, Man, and Cybernetics — Part B: Cybernetics, 21. 452–456.
5. Lin, D.T., Computer Access Authentication with neural network based keystroke identity verification. in International Conference on Neural Networks, (Houston, Texas, 1997), 174–178.
6. Marcus Brown and Rogers, S.J. User Identification via Keystroke Characteristics of typed names using Neural Networks. International Journal of Man-Machine Studies, 39. 999–1014.
7. Obaidat, M.S., A verification methodology for computer systems users. in Proceedings of the 1995 ACM Symposium on Applied Computing, (Nashville, Tennessee, 1995), ACM Press, 258–262.
8. D. Umphress and Williams, G. Identity verification through keyboard characteristics. Int. J. Man-Machine Studies, 23 (3). 263–273.
9. J. Leggett and Williams, G. Verifying identity via keystroke characteristics. International Journal of Man-Machine Studies, 28 (1). 67–76
10. R. Gaines, W. Lisowski, S. Press and Shapiro, N. Authentication by Keystroke Timing: Some Preliminary Results Tech. report R-256-NSF, Tech report R-256-NSF, RAND, Santa Monica, CA, 1980.
11. Rick Joyce and Gupta, G. Identity Authentication Based on Keystroke Latencies. Communications of the ACM, 33 (2). 168–176.
12. Shrijit S. Joshi and Phoha, V.V., Investigating Hidden Markov Models capabilities in Anomaly Detection. in 43rd ACM SE Conference, (Kennesaw State University, Kennesaw, Georgia, USA, March 2005), ACM.
13. Vinar, T. Enhancements to Hidden Markov Models for Gene Finding and Other Biological Applications Computer Science, University of Waterloo, Waterloo, Ontario, Canada, 2005, 162.
14. Yong Sheng, Vir V. Phoha and Rovnyak, S.M. A Parallel Decision Tree-Based Method for User Authentication Based on Keystroke Patterns. IEEE Transactions on Systems, Man, and Cybernetics — Part B: Cybernetics, 35 (4). 826–833.
15. Sampath Vuyyuru, Vir V. Phoha, Shrijit S. Joshi, Shashi Phoha, and A. Ray, «Computer User Authentication using Hidden Markov Model through Keystroke Dynamics», Manuscript submitted to ACM Transactions on Information and System Security, 2006.
16. Иванов А. И. Биометрическая идентификация личности по динамике подсознательных движений. //Монография. Пенза. Изд-во ПГУ, 2000 г., 178 с.
17. Чалая Л. Э. Модель идентификации пользователей по клавиатурному почерку //Искусственный интеллект. —2004. — № 4. — С. 811–817.
18. Абашин В. Г. Определение психофизиологического состояния оперативного персонала по клавиатурному почерку на нефтеперерабатывающих мини-заводах [Электронный ресурс] / В. Г. Абашин, А. И. Суздальцев, В. А. Лобанова // Электронный журнал «Нефтегазовое дело», 2006. http://www.ogbus.ru/authors/Suzdaltsev/Suzdaltsev_1.pdf
19. Bleha, S., Slivinsky, C., Hussien, B.: Computer-access security systems using keystroke dynamics. IEEE Transactions on Pattern Analysis and Machine Intelligence 12 (1990) 1217–1222
20. Obaidat, M.S., Sadoun, B.: Verification of computer users using keystroke dynamics. IEEE Transactions on Systems, Man and Cybernetics 27 (1997) 261–269
21. Shepherd, S.J.: Continuous authentication by analysis of keyboard typing characteristics. In: European Convention in Security and Detection, Brighton, UK, Bradford University (1995) 111–114
22. John A. Robinson, Vicky M. Liang, J. A. Michael Chambers and Mackenzie, C. L. Computer user verification using login string keystroke dynamics. IEEE Transactions on Systems, Man and Cybernetics — Part A: Systems and Humans, 28 (2). 236–241.
23. M. S. Obaidat and Sadoun, B. Verification of Computer Users Using Keystroke Dynamics. IEEE Transactions on Systems, Man, and Cybernetics — Part B: Cybernetics, 27 (2). 261–269.
24. Phoha, V.V., Kumar, P. and Vuyyuru, S. K. Keystroke Typing Rhythm as an Input Vector for Authentication. Manuscript under revision for submission to IEEE Transactions on Systems, Man and Cybernetics, Part B.
25. D. Umphress and Williams, G. Identity verification through keyboard characteristics. Int. J. Man-Machine Studies, 23 (3). 263–273.
26. F. Monroe and Rubin, A., Authentication via keystroke dynamics. in Proceedings of ACM Workshop, (1997), ACM, 48–56.
27. J. Leggett, G. Williams, M. Usnick and Longnecker, M. Dynamic identity verification via keystroke characteristics. International Journal of Man-Machine Studies (35). 859–870.

28. Yong Sheng, Vir V. Phoha and Rovnyak, S.M. A Parallel Decision Tree-Based Method for User Authentication Based on Keystroke Patterns. IEEE Transactions on Systems, Man, and Cybernetics — Part B: Cybernetics, 35 (4). 826–833.
29. Разработка и исследование методов скрытого клавиатурного мониторинга: автореф. дис. на соиск. учен. степ. канд. техн. наук: спец. 05.13.19 / Казарин Максим Николаевич; Таганрогский гос. радиотех. ун-т. — Таганрог: 2006.
30. Идентификация пользователя ЭВМ и автора программного продукта: метод. рекомендации / А. Ю. Комиссаров, А. В. Подлесный; Эксперт.-криминалист. центр. — Москва: 1996. — 39 с.

© Швырев Борис Анатольевич (bor2275@yandex.ru).

Журнал «Современная наука: актуальные проблемы теории и практики»



Научно-исследовательский институт ФСИИ России