Лаба 1.

ФИО

Преображенский А.А. (группа 6111)
Чекулаев Д.О. (группа 6111)

Topic

User Authentication; Biometry; Touch Screens

Описание предметной области

Данный топик охватывает исследования в области аутентификации пользователя, биометрии и сенсорный дисплей. User Authentication - это процесс проверки подлинности, во время которого определяется достоверность введённых в специально предназначенные поля данных. Обычно речь идёт о логине и пароле. Аутентификация, при помощи биометрии – один из методов идентификации пользователя. Touch Screen – это сенсорный экран, который позволяет взаимодействовать с устройством с помощью касаний пальцем или стилусом. Простыми словами – это сенсорная панель, которая работает от прикосновений: вы управляете элементами на экране или пальцами, или специальным пером.

Недостаток (gap)

Биометрические машины далеки от совершенства. Частота технических ошибок в некоторых случаях настолько велика, что создает большой хаос для всей системы безопасности. Главная проблема нынешних аутентификационных систем - безопасность. Частые взломы и утечки баз данных играют на руку злоумышленникам, которые не пренебрегают краденными данными.

Идея

Усовершенствование конфиденциальности баз данных, содержащих аутентификационную информацию. Разработка новых программ-фаерволов для защиты данных пользователей, а также оптимизация систем для большей доступности.

В частности, мы бы хотели предложить создание новейшей системы аутентификации, основанной на человеческой ДНК (DNA auth). Подразумевается получение доступа к какой-либо системе пользователем, с помощью его ДНК.

Для большей защиты данных пользователя предлагаем создание фаервола, основанного на мощнейших вирусах (Plague Attack). Злоумышленник, который пытается получить доступ к чужим данным, будет подвергнут мощнейшей вирус-атаке.

Краткий текст обзора

В настоящее время существует несколько методов проверки личности человека или устройства,
которые обеспечивают безопасность и защиту от несанкционированного доступа [1], [2].

Многофакторная аутентификация (MFA) требует двух или более форм подтверждения личности [3]. Это более безопасный метод, так как он затрудняет злоумышленникам получение доступа. Примеры форм MFA включают комбинацию пароля и ключа безопасности или отпечатка пальца [3], [4].

Биометрическая аутентификация использует уникальные биологические характеристики человека [7], такие как отпечаток пальца, радужная оболочка глаза, голос и лицо, для подтверждения личности [3], [5], [6], [7].
Этот метод обеспечивает высокую степень безопасности, так как физические черты человека сложно подделать.

Физиологическая биометрия использует измерения, связанные с человеческим телом, такие как отпечатки пальцев, сканирование глаз и распознавание лиц [7].
Поведенческая биометрия аутентифицирует пользователей на основе измерений, связанных с их поведением, таких как распознавание голоса и нажатия клавиш [5],
которые являются примерами поведенческой биометрии [8].

Многие системы аутентификации объединяют несколько биометрических методов для обеспечения большей надежности. Это называется мультимодальными системами [7], [9].

Биометрическая аутентификация обеспечивает высокий уровень безопасности, точности и удобства [9]. Однако у нее есть недостатки, такие как высокая стоимость, возможность ошибок и сложность в реализации [10].

Так как системы аутентификации несовершенны, необходимо обратить внимание на физическую неподвижность биометрических данных и риск их утечки или взлома [3], следует учитывать частоту ошибок и задержек, которые могут возникнуть при использовании устройств [8].

Таким образом, приведённый список статей отражает актуальность данного топика и отражает проблемы биометрических систем. Создание и внедрение новейшей системы аутентификации, основанной на человеческой ДНК (DNA auth) (подразумевается получение доступа к какой-либо системе пользователем, с помощью его ДНК) и создание фаервола, основанного на мощнейших вирусах (Plague Attack) (злоумышленник, который пытается получить доступ к чужим данным, будет подвергнут мощнейшей вирус-атаке) поможет системам биометрической идентификации пользователей выйти на новый уровень безопасности.

References

[1] M. Papathanasaki, L. Maglaras, и N. Ayres, «Modern Authentication Methods: A Comprehensive Survey», *AI Comput. Sci. Robot. Technol.*, т. 2022, сс. 1–24, июн. 2022, doi: 10.5772/acrt.08.

[2] C. J. Kroeze и K. M. Malan, «User Authentication based on Continuous Touch Biometrics», *South Afr. Comput. J.*, т. 28, вып. 2, Art. вып. 2, дек. 2016, doi: 10.18489/sacj.v28i2.374.

[3] J. Angulo и E. Wästlund, «Exploring Touch-Screen Biometrics for User Identification on Smart Phones», в *Privacy and Identity Management for Life*, т. 375, J. Camenisch, B. Crispo, S. Fischer-Hübner, R. Leenes, и G. Russello, Ред., в IFIP Advances in Information and Communication Technology, vol. 375. , Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, сс. 130–143. doi:

10.1007/978-3-642-31668-5_10.
[4] H. Dozono, T. Inoue, и M. Nakakun, «A study of the Graphical User Interfaces for Biometric Authentication System», *Study Graph. User Interfaces Biom. Authentication Syst.*, т. 1, сс. 1–6.
[5] P. Kałużny, «Touchscreen Behavioural Biometrics Authentication in Self-contained Mobile Applications Design», в *Business Information Systems Workshops*, т. 373, W. Abramowicz и R. Corchuelo, Ред., в Lecture Notes in Business Information Processing, vol. 373. , Cham: Springer International Publishing, 2019, сс. 672–685. doi: 10.1007/978-3-030-36691-9_56.
[6] M. Antal и L. Z. Szabó, «Biometric Authentication Based on Touchscreen Swipe Patterns», *Procedia Technol.*, т. 22, сс. 862–869, 2016, doi: 10.1016/j.protcy.2016.01.061.
[7] S. Phadke, «The Importance of a Biometric Authentication System», *SIJ Trans. Comput. Sci. Eng. Its Appl. CSEA*, т. 1, вып. 4, Art. вып. 04, окт. 2013, doi: 10.9756/SIJCSEA/V1I4/0104550402.
[8] A. Ibrahim, «Data Science Solution for User Authentication», *Data Sci. Solut. User Authentication*, т. 1, сс. 1–97, июл. 2017.
[9] C.-S. Koong, T.-I. Yang, и C.-C. Tseng, «A User Authentication Scheme Using Physiological and Behavioral Biometrics for Multitouch Devices», *Sci. World J.*, т. 2014, сс. 1–12, 2014, doi: 10.1155/2014/781234.
[10] P. Kumar, «Touch Screen Based Authentication», т. 5, вып. 7, Art. вып. 7, 2013.