МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ "МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ Н.Э. БАУМАНА (НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)"

«БЕЗОПАСНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ»

ДЕСЯТАЯ
МЕЖДУНАРОДНАЯ
НАУЧНО-ТЕХНИЧЕСКАЯ КОНФЕРЕНЦИЯ

(Москва, 3-4 декабря 2019 года)

СБОРНИК ТРУДОВ КОНФЕРЕНЦИИИ

МГТУ им.Н.Э.Баумана
НУК «Информатика и системы управления»
МОСКВА-2019

УДК 003.26.7: 004.05
ББК 32.937.202
Б31

Б31

Безопасные информационные технологии. Сборник трудов Десятой международной научно-технической конференции – М.: МГТУ им. Н.Э. Баумана, 2019. 409 с. – илл.

ISBN 978-5-9906630-6-0

Сборник содержит тезисы докладов, представленных на Десятой всероссийской научно-технической конференции "Безопасные информационные технологии" (БИТ-2019), проходившей 3-4 декабря 2019 г. в Москве в МГТУ им. Н.Э. Баумана.

Тезисы публикуются в редакции научных руководителей или в авторской редакции при наличии ученой степени.

УДК 004.056.52

Методы аутентификации с использованием носимых устройств

Ванин А.В.[42]

Аннотация. *Обоснована актуальность изучения методов аутентификации с использованием носимых устройств на основе результатов осуществленного патентного поиска в отечественном и зарубежном сегментах. Предложена классификация методов аутентификации с использованием носимых устройств на основе факторов владения (токен), знания (пароль) и сущности (биометрия). Приведены примеры наиболее современных методов аутентификации с использованием таких носимых устройств как умные часы, очки, кольца. Сделан вывод относительно перспектив дальнейшего развития области изучения и разработки схем и методов аутентификации с использованием носимых устройств.*

Ключевые слова. *Схемы и методы аутентификации, патентный поиск, умные часы, умные очки, умное кольцо, смартфон.*

Введение

Процедура аутентификации может представлять определенные трудности для пользователя становясь чрезмерно отягощенной [1]. В этом случае своеобразным компенсирующим средством выступают методы аутентификации с использованием носимых устройств (умные часы, очки, браслеты, кольца, одежда), гарантирование безопасности которых также является актуальной задачей [2].

Патентный поиск и классификация

Актуальность и перспективность изучения подтверждается проведенным в соответствии с ГОСТ Р. 15.011-96 патентным поиском (цифры актуальны на ноябрь 2019 года). По данной тематике и схожей с ней в отечественном патентном сегменте подано 56 заявок (на основе данных ФИПС), несоизмеримо большее количество в зарубежном – 43241 (на основе данных Google Patents).

Основой классификации методов аутентификации с использованием носимых устройств может выступать схема, разделяющая техники аутентификации на те, которые подчинены факторам: собственности («то, чем владеешь» / токен), знания («то, что знаешь» / пароль) и сущности («то, чем являешься» / биометрия).

Токен

Система аутентификации концептуально схожая использованию физических ключа и замка предложена в работе [3]. В ней обладатель умных часов, содержащих доверенный сертификат, аутентифицируется через мобильный терминал путем прикладывания к нему часов. Сертификат исследуется терминалом на предмет в предоставлении/отказе авторизованного уровня доступа.

С целью оптимизации данной схемы Corner и Noble [4] предложена парадигма аутентификации нулевого взаимодействия, в которой используется активный токен, автономно собирающий доверительные сертификаты и связывающийся с устройством пользователя через беспроводную связь малой дальности. Южнокорейские коллеги [5] предлагают схожую схему, использующую при этом комбинацию смарт-часов и мобильного телефона. В ней пользователь получает авторизацию для совершения защищенных онлайн-транзакций до тех пор, пока оснащенные NFC смарт-часы связаны с мобильным устройством [6].

[42] Ванин Александр Владимирович, магистрант МГТУ им. Н.Э. Баумана, г. Москва, эл. почта: vaninav@student.bmstu.ru

В работе [7] предлагается носимый ключ, базирующийся на передаче сигналов через тело пользователя, аутентифицирующее его в случае прикосновения к устройству. Похожее решение, основанное на инфракрасном излучении предложено немецкими исследователями [8]. Пользователь – обладатель кольца осуществляет прикосновение к настольному экрану, в результате чего передаются псевдослучайные битовые последовательности, декодируемые дисплеем длтя осуществления аутентификации.

Пароль

Личные дисплеи при использовании умных очков исследуются в работе D. Yadav [9], сопоставляя проверки подлинности через прикосновение или голос с выводом изображения на экран устройства.

Аналогично, P. Chan [10] представил схему аутентификации для разблокировки умных очков, когда QR-код продуцирован на смартфон пользователя и его сканирование осуществляется с использованием встроенной камеры.

J. Thorpe [11] изучает, каким образом могут существовать технологии интерфейсов объединяющих мозг человека и его персональное устройство, используя ввод пароля как основной механизм аутентификации.

Биометрия

Классифицируется на методы: 1) явные, направленные на измерение врожденных характеристик пользователя; 2) имплицитные, осуществляющие сбор данных с устройства пользователя в «скрытом» режиме; 3) носимые системы аутентификации, соединяющие в себе явные и имплицитные составляющие.

Современные разработки с применением устройств типа умных очков обращаются к распознаванию радужной оболочки глаз [12].

J. Yang [13] предлагает приложение, собирающее данные относительно движений от надетого на запястье устройства в процессе воспроизведения жестов с целью идентификации. В пространстве мобильных приложений также разрабатываются имплицитные методы аутентификации пользователя [14]. Данная череда исследований базируется на парадигме непрекращающейся аутентификации, основанной на поведенческой биометрии, получившая название сенсорно-обусловленной аутентификации [15]. Источником для нее служат: данные, извлекаемые с датчиков, прикрепленных к телу пользователя (например, с сенсоров движения); данные, собираемые в процессе активного взаимодействия пользователя с персональным устройством (например, с экраном смартфона).

Исследуются также возможности аутентификации, основанной на параметрах температуры тела пользователя с использованием умных часов и аппарата нейронных сетей [16].

Предлагаются методы реализации процесса аутентификации посредством анализа частоты сердечных сокращений с использованием датчика ЭКГ при использовании комбинации смартфона и умных часов [17].

Наконец, разработка «BreathPrint» [18], представляет схему, основанную на акустических особенностях дыхания человека [19, 20], снимаемых обычным микрофоном смартфона.

Выводы

Несмотря на то, что аутентификация с использованием носимых устройств представляет только зарождающийся исследовательский интерес, комбинация носимых технологий с мобильными платформами уже сегодня предоставляет новые возможности по причине увеличивающихся вычислительной мощности и интерактивных возможностей. Скорее, чем служить в качестве обычных токенов, носимые устройства, несомненно, будут играть в ближайшем будущем значительную роль в реализации эффективных многофакторных схем аутентификации.

Литература

1. Барабанов А.В. и др. Семь безопасных информационных технологий - М.: ДМК Пресс, 2017. 224 с.
2. Das, Ashok Kumar (2017). Lightweight authentication protocols for wearable devices / Ashok Kumar Das, Sherali Zeadally, Mohammad Wazid // Computers & Electrical Engineering. Volume 63 (pp. 196-208).
3. Al-Muhtadi, J., Mickunas, M. D., & Campbell, R. H. (2001). Wearable security services. In Proceedings 21st International Conference on Distributed Computing Systems Workshops (pp. 266–271).
4. Corner, M. D., & Noble, B. D. (2002). Zero-interaction authentication. In Proceedings of the 8th annual international conference on Mobile computing and networking (pp. 1–11).
5. Cha, B.-R., Lee, S.-H., Park, S.-B., Lee, G.-K., & Ji, Y.-K. (2015). Design of Micro-payment to Strengthen Security by 2 Factor Authentication with Mobile & Wearable Devices. In Security, Reliability, and Safety 2015 (pp. 28–32).
6. Рабинович А.С., Казарин О.В. Методика аутентификации пользователя в информационной системе с использованием технологии NFC // Вопросы кибербезопасности. 2013. № 2 (2). С. 59-62.
7. Matsushita, N., Tajima, S., Ayatsuka, Y., & Rekimoto, J. (2000). Wearable key: device for personalizing nearby environment. In Digest of Papers. Fourth International Symposium on Wearable Computers (pp. 119–126).
8. Roth, V., Schmidt, P., & Güldenring, B. (2010). The IR ring: authenticating users' touches on a multi-touch display. In Proceedings of the 23nd annual ACM symposium on User interface software and technology (pp. 259–262).
9. Yadav, D. K., Ionascu, B., Ongole, S. V. K., Roy, A., & Memon, N. D. (2015). Design and Analysis of Shoulder Surfing Resistant PIN based Authentication Mechanisms on Google Glass. In International Conference on Financial Cryptography and Data Security (pp. 281–297).
10. Chan, P., Halevi, T., & Memon, N. D. (2015). Glass OTP: Secure and Convenient User Authentication on Google Glass. In International Conference on Financial Cryptography and Data Security (pp. 298–308).
11. Thorpe, J., Oorschot, P. C. van, & Somayaji, A. (2005). Pass-thoughts: authenticating with our minds. In Proceedings of the 2005 workshop on New security paradigms Vol. 2005 (pp. 45–56).
12. Li, Y.-H., & Huang, P.-J. (2017). An Accurate and Efficient User Authentication Mechanism on Smart Glasses Based on Iris Recognition. Mobile Information Systems (pp. 1–14).
13. Yang, J., Li, Y., & Xie, M. (2015). MotionAuth: Motion-based authentication for wrist worn smart devices. In 2015 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops) (pp. 550–555).
14. Luca, A. D., Hang, A., Brudy, F., Lindner, C., & Hussmann, H. (2012). Touch me once and I know it's you!: implicit authentication based on touch screen patterns. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 987–996).
15. Shen, C., Chen, Y., & Guan, X. (2018). Performance evaluation of implicit smartphones authentication via sensor-behavior analysis. Information Sciences, 430, (pp. 538–553).
16. Enamamu, T. S., Clarke, N., Haskell-Dowland, P., & Li, F. (2017). Smart watch based body-temperature authentication. In 2017 International Conference on Computing Networking and Informatics (ICCNI) (pp. 1–7).
17. Kang, S. J., Lee, S. Y., Cho, H. I., & Park, H. (2016). ECG Authentication System Design Based on Signal Analysis in Mobile and Wearable Devices. IEEE Signal Processing Letters, 23(6) (pp. 805–808).
18. Chauhan, J., Hu, Y., Seneviratne, S., Misra, A., Seneviratne, A., & Lee, Y. (2017). BreathPrint: Breathing Acoustics-based User Authentication. In Proceedings of the 15th Annual International Conference on Mobile Systems, Applications, and Services (pp. 278–291).
19. Горшков Ю.Г. Акустографическое исследование звуков сердца и легких с оценкой эмоциональной напряженности пациента по голосу. В сборнике: Биотехнические, медицинские, экологические системы и робототехнические комплексы - Биомедсистемы-2017 сборник трудов

XXX Всероссийской научно-технической конференции студентов, молодых ученых и специалистов. Рязанский государственный радиотехнический университет. 2017. С. 163-166.
20. Устройство оценки эмоциональной напряженности человека по голосу / Горшков Ю.Г. и др. - Патент на полезную модель RUS 165114 14.09.2015. 2016.

Научный руководитель. *Цирлов Валентин Леонидович, кандидат технических наук, доцент кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана, v.tsirlov@bmstu.ru*

Authentication methods using wearable devices

Vanin A.V.[43]

Abstract. *The relevance of the study of authentication methods using wearable devices based on the results of the patent search in the domestic and foreign segments is substantiated. The classification of authentication methods using wearable devices based on the factors of ownership (token), knowledge (password) and entity (biometrics) is proposed. Examples of the most modern authentication methods using such wearable devices as smartwatches, glasses, rings are given. The conclusion is made regarding the prospects for further development of the field of study and development of methods of authentication using wearable devices.*

Keywords. *Authentication schemes and methods, patent search, smartwatch, smart ring, smart glasses, smartphone.*

[43] Vanin Alexander Vladimirovich, graduate student, Bauman Moscow State Technical University, Moscow, e-mail: vaninav@student.bmstu.ru

ОГЛАВЛЕНИЕ