ФИЗИКА ЭЛЕМЕНТАРНЫХ ЧАСТИЦ И АТОМНОГО ЯДРА
2024. Т. 55, вып. 3. С. 722–727

НЕПРЕРЫВНАЯ АУТЕНТИФИКАЦИЯ В СИСТЕМАХ ИНТЕРНЕТА ВЕЩЕЙ

*Ю. С. Матюшин *, В. В. Корхов*

Санкт-Петербургский государственный университет, Санкт-Петербург, Россия

Непрерывная аутентификация — это новый подход к аутентификации пользователей в распределенных системах. Его главный принцип состоит в том, что, в отличие от «традиционного подхода», в котором пользователь проходит процедуру аутентификации только в начале сессии, личность пользователя повторно верифицируется на протяжении всей сессии. Рассматриваются методы непрерывной аутентификации в распределенных системах, которые могут быть использованы в системах интернета вещей. В них используются технологии блокчейна, машинного обучения и биометрии. На основе результатов анализа предлагается общая схема работы перспективного алгоритма непрерывной аутентификации.

Continuous authentication (CA) is a new approach to user authentication in distributed systems. Its main principle is that unlike a “traditional” approach, where a user is only authenticated once at the beginning of a session, the user’s identity is re-verified throughout the entire session. Distributed system continuous authentication algorithms that can be used with Internet of Things systems are investigated. They include methods using such technologies as blockchain, machine learning, and biometrics. Based on the results of the analysis, a prospective CA algorithm is outlined.

PACS: 89.20.Ff

ВВЕДЕНИЕ

Аутентификация является необходимой частью архитектуры безопасности любой распределенной системы. Примером ее важности может послужить исследование [1], согласно которому до 80 % утечек данных за последние годы были связаны с какой-либо уязвимостью в механизме аутентификации.

В традиционных, или «статических», механизмах безопасности пользователь проходит процедуру аутентификации только один раз, в начале своего взаимодействия с системой. Но с этим связана важная проблема: после успешного прохождения аутентификации пользователь получает доступ к системе вплоть до конца сеанса, и, если контроль над устрой-

* E-mail: st086397@student.spbu.ru

ством пользователя был перехвачен злоумышленником уже после начала сеанса, проверить это невозможно.

Для борьбы с данной уязвимостью был создан новый подход под названием непрерывной аутентификации. Его главная идея — подтверждать личность пользователя не один раз, в начале его взаимодействия с системой, а многократно в течение всего сеанса.

Системы интернета вещей (IoT) становятся все более и более распространенными и вместе с тем постоянно усложняются; из-за этого становится более острой и необходимость обеспечить их безопасность, что подразумевает в том числе и надежные механизмы аутентификации. С другой стороны, имплементация данных механизмов в системах интернета вещей также связана с некоторыми уникальными проблемами.

В данной статье рассмотрены алгоритмы непрерывной аутентификации, которые могут быть применены в системах IoT. На основе сравнительного анализа предложены характеристики потенциального нового подхода к аутентификации в контексте IoT, а также направления будущих исследований.

МЕХАНИЗМЫ АУТЕНТИФИКАЦИИ ДЛЯ СИСТЕМ ИНТЕРНЕТА ВЕЩЕЙ

В статье [2] нами были определены самые распространенные в настоящее время алгоритмы непрерывной аутентификации: использование клавиатурного почерка, формы лица, движений мыши, взаимодействия с тачскрином, а также действий пользователя в системе.

Однако с интернетом вещей связаны несколько уникальных проблем для аутентификации пользователей. В частности, IoT-устройства, как правило, обладают ограниченными вычислительными ресурсами и памятью, следовательно, ресурсоемкие методы не являются оптимальными в подобной среде. Другие ограничения связаны с энергопотреблением и пропускной способностью сети, что требует выбирать более «легкие» методы. Наконец, большинство упомянутых выше подходов к аутентификации требуют использования устройств ввода, которые отсутствуют во многих IoT-устройствах.

На основе анализа публикаций с учетом вышеупомянутых ограничений мы определили несколько методов непрерывной аутентификации, которые могут быть использованы в среде IoT. Ниже приведены их краткие характеристики.

CAB-IoT [3] — это метод аутентификации на основе блокчейна, предназначенный для использования в среде интернета вещей. Метод является распределенным и использует «туманные узлы» для аутентификации с помощью смарт-контрактов, записанных в децентрализованном реестре. Это позволяет CAB-IoT обойти упомянутые нами вычислительные ограничения и реализовать аутентификацию, не полагаясь на третью сторону. В качестве блокчейна используется Ethereum, выбранный из-за

возможности присвоения уникального адреса Ethereum каждому узлу, а также высокой скорости транзакций. Для аутентификации пользователя используется ML-технология распознавания лиц, при этом система аутентификации присваивает результату «балл доверия», и, если этот балл достаточно высок, пользователю предоставляется доступ, что фиксируется в распределенном реестре.

WiFiU [4] — это метод динамической биометрии, основанный на походке. Под «динамическими» понимаются методы, использующие модель поведения человека (разговор, набор текста, походка и т. д.) в качестве уникальной характеристики, позволяющей подтвердить личность пользователя; они отличаются от статических методов, основанных на неизменных характеристиках (отпечатки пальцев, форма лица и т. д.). Для аутентификации пользователя WiFiU использует его походку. Для этого не нужны ни камеры, ни датчики пола, а только передатчик и приемник WiFi. Движения человека уникальным образом влияют на такие характеристики, как CSI (информация о состоянии канала) и RSS (уровень принимаемого сигнала). Система изучает особенности походки различных пользователей и использует их для подтверждения личности.

Чуан и др. [5] разработали гибридный легкий протокол, сочетающий статическую и непрерывную аутентификации. В отличие от предыдущих методов в данном случае речь идет об аутентификации устройства, а не пользователя. Для этого устройство и «шлюз» (орган аутентификации) обмениваются некоторым секретом в ходе инициализации. Затем, на этапе статической аутентификации, устройство верифицируется с помощью криптографического метода, основанного на общем секрете. В ходе взаимодействия устройство регулярно посылает «шлюзу» сообщения, а для непрерывной аутентификации используются такие параметры, как временны́е метки и время работы устройства от аккумулятора.

PUFDCA [6] также является гибридным методом аутентификации устройств. Статическая часть метода использует PUF (physical unclonable function) — уникальную характеристику каждого устройства. Если статическая аутентификация проходит успешно, начинается сеанс, а для проверки местоположения устройства в качестве метода аутентификации используются измерения CSI; если устройство пытается подключиться из необычного места или время сеанса заканчивается, то метод возвращается к статической аутентификации.

ZASH [7] (Zero-Aware Smart Home system) был разработан для использования в «умных домах», где могут встречаться различные типы пользователей с разными правами доступа (например, взрослые и дети). Таким образом, она сочетает в себе аутентификацию — подтверждение личности пользователя — и авторизацию — принятие решения о том, имеет ли данный пользователь право доступа к той или иной части системы. Система непрерывной аутентификации оценивает поведение

пользователя, используя различные контекстные подсказки (время доступа, используемое устройство и т. д.). Если поведение пользователя нарушает установленную модель, то система переходит к статической аутентификации — сканированию отпечатков пальцев.

В таблице представлен сравнительный анализ перечисленных методов.

Сравнительный анализ методов непрерывной аутентификации

Метод	Принцип работы	Достоинства	Недостатки
CAB-IoT (2020)	Распознавание лиц и распределенный реестр	Ограниченные требования к пропускной способности и памяти, ресурсоемкие процессы вынесены на «туманные узлы», высокая точность распознавания	Недостаточное тестирование, требуется картинка лица, требуются «туманные узлы»
WiFiU (2017)	Походка пользователя	Не требует специальных устройств и освещения, легче развертывать и больше покрытия по сравнению с методами, основанными на видеокамерах	Дистанция распознавания 6 м, ограниченная точность, только один пользователь, необходимы движения
Чуан и др. (2018)	Статическая аутентификация с использованием общего секрета и непрерывная с использованием заряда батареи и временны́х меток	Легкая криптография, учитывающая ограниченные вычислительные ресурсы и память	Необходимы фаза инициализации, безопасное хранилище секретов, частые сообщения
PUFDCA (2022)	Статическая аутентификация с использованием PUF, непрерывная с использованием расположения устройства	Легкий метод с низким потреблением ресурсов, устойчив ко многим разновидностям атак	Необходимы статическая аутентификация перед каждым сеансом и безопасная среда
ZASH (2021)	Контекстные подсказки и биометрия	Гибкий метод со множеством уровней доступа, защита от попыток имитации пользователя	Необходимы неизменные модели поведения пользователей

ВЫВОДЫ

На основе существующих методов можно выделить несколько характеристик потенциального механизма аутентификации:

- *распределенность* — такой метод будет масштабируемым и подойдет для системы любого размера;
- *биометрия* — большинство перечисленных методов являются биометрическими, что позволяет осуществлять непрерывную аутентификацию, не мешающую работе пользователя;
- *гибридность* — непрерывная аутентификация дополняет статическую, но не заменяет ее;
- *использование контекста* — в частности, местоположения пользователя и контекстных подсказок;
- *типизация пользователей* — как в «умных домах», так и в корпоративных системах, что позволяет сделать систему более гибкой.

На рисунке показан высокоуровневый обзор потенциального алгоритма.

Дальнейшие исследования могут включать в себя изучение биометрических технологий, наиболее применимых для непрерывной аутентификации в среде интернета вещей, и распределенных технологий, подходящих для данной среды. Поскольку все исследованные нами алгоритмы имеют существенные недостатки, необходимо разработать новый алгоритм, основанный на их лучших, по нашему мнению, характеристиках.

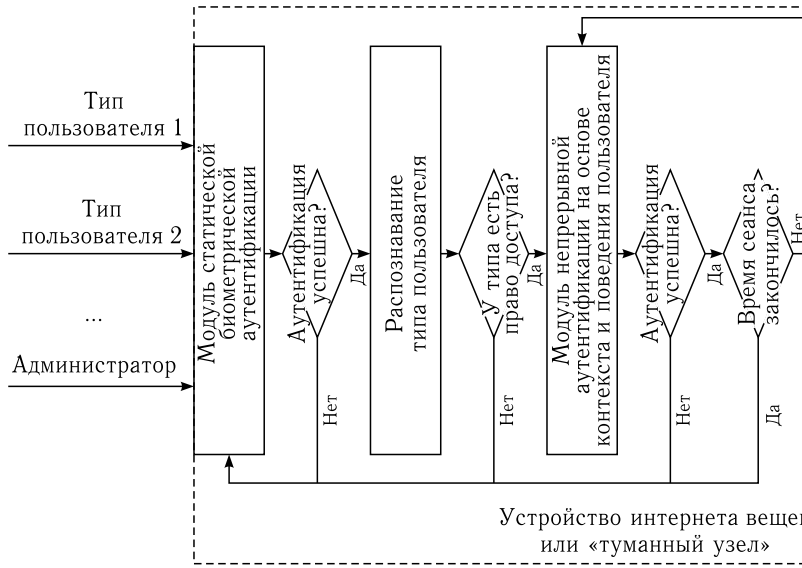

Схема работы перспективного алгоритма непрерывной аутентификации

Работа выполнена при поддержке Санкт-Петербургского государственного университета, проект 94062114.

СПИСОК ЛИТЕРАТУРЫ

1. Verizon 2022 Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/dbir/2022/master-guide/ (accessed 10.09.2023).
2. *Matiushin I., Korkhov V.* Continuous Authentication Methods for Zero-Trust Cybersecurity Architecture // Proc. of Comput. Science and Its Applications Workshops (ICCSA 2023), Athens, July 3–6, 2023. P. 334–351; doi: 10.1007/978-3-031-37120-2_22.
3. *Al-Naji F., Zagrouba R.* CAB-IoT: Continuous Authentication Architecture Based on Blockchain for Internet of Things // J. King Saud Univ. Comput. Inform. Sci. 2020. V. 34. P. 2497–2514; doi: 10.1016/j.jksuci.2020.11.023.
4. *Shahzad M., Singh M. P.* Continuous Authentication and Authorization for the Internet of Things // IEEE Internet Comput. 2017. V. 21. P. 86–90; doi: 10.1109/MIC.2017.33.
5. *Chuang Y.-H. et al.* A Lightweight Continuous Authentication Protocol for the Internet of Things // Sensors. 2018. V. 18; doi: 10.3390/s18041104.
6. *Alshomrani S., Li S.* PUFDCA: A Zero-Trust-Based IoT Device Continuous Authentication Protocol // Wireless Commun. & Mobile Comput. 2022. V. 2022. P. 1–9; doi: 10.1155/2022/6367579.
7. *Silva G., Macedo D., Santos A.* Zero Trust Access Control with Context-Aware and Behavior-Based Continuous Authentication for Smart Homes // Proc. Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais. 2021. P. 43–56; doi: 10.5753/sbseg.2021.17305.