УДК 004.89:004.056

Пуйко Д.Д.
Северо-Кавказский федеральный университет, Ставрополь

Научный руководитель:
Петренко В.И.
Северо-Кавказский федеральный университет, Ставрополь

ПРОБЛЕМЫ МНОГОФАКТОРНОЙ АУТЕНТИФИКАЦИИ В ДЕЦЕНТРАЛИЗОВАННЫХ КИБЕРФИЗИЧЕСКИХ СИСТЕМАХ

Аннотация. Многофакторная аутентификация (MFA) имеет первостепенное значение для обеспечения безопасности киберфизических систем (CPS), особенно в сфере Интернета вещей (IoT), характеризующейся ограниченными ресурсами устройств и критически важными операциями. Обсуждаются возможные стратегии смягчения последствий, включающие легковесную криптографию, вычисления вне цепи, специализированные механизмы консенсуса и надежные протоколы децентрализованного управления. Трудность заключается в обеспечении баланса между надежной безопасностью, удобством использования и производительностью в условиях жестких ограничений этих децентрализованных сред IoT.

Ключевые слова: многофакторная аутентификация (MFA), Интернет вещей (IoT), киберфизические системы (CPS), блокчейн.

Киберфизические системы (CPS) представляют собой тесную интеграцию вычислений, сетей и физических процессов. Интернет вещей (IoT) является ярким проявлением CPS, объединяющим миллиарды устройств – от простых датчиков и исполнительных механизмов до сложных машин и носимых устройств – часто работающих в условиях значительных ограничений ресурсов (вычислительной мощности, памяти, энергии) и взаимодействующих с физическим миром, часто в таких критически важных приложениях, как промышленный контроль (IIoT) или здравоохранение (IoHT). Обеспечение безопасности таких систем имеет огромное значение, поскольку уязвимости могут привести к физическому ущербу, утечке данных или нарушению работы основных служб.

Многофакторная аутентификация (MFA) – это краеугольный камень современной системы безопасности, требующий от пользователей или организаций предоставления нескольких доказательств (факторов) из разных категорий – знания (то, что вы знаете), владения (то, что у вас есть) и принадлежности (то, что вы есть) – для подтверждения их личности. Реализация MFA в IoT крайне важна, но сложна из-за ограничений устройств и масштабов развертывания.

Как отмечается в работе [1], посвященной многофакторной аутентификации в контексте Интернета вещей, для обеспечения безопасности таких систем необходимо решить ряд следующих вопросов:

– как взвесить факторы?

– как адаптировать решения?

– как завоевать доверие пользователей?

– как безопасно получить внешние данные?

Первая проблема при проектировании моделей многофакторной аутентификации заключается в отсутствии общепринятых критериев для ранжирования аутентификационных факторов и выбора метрик их эффективности. Это приводит к необъективности приоритезации факторов и контекстной зависимости.

Вторая проблема уже частично решается системами с использованием статистических моделей, основанных на байесовских сетях [2] или нейронных сетях [3]. Однако в контексте IoT-устройств с низким энергопотреблением она сохраняет актуальность, так как эти методы требуют значительных вычислительных мощностей для обучения и инференса моделей, больших объемов памяти для хранения параметров (например, весов нейросетей), постоянной энергии для обработки данных в реальном времени.

Третья проблема касается необходимости прозрачности модели многофакторной аутентификации. Ключевой вызов – обеспечение доверия к системе через описание ее решений, особенно в сценариях, где факторы аутентификации динамически меняются.

В четвертой проблеме затрагиваются риски взаимодействия между устройствами, создающих уязвимости, связанные с отсутствием гарантий надежности и целостности внешних источников. Это требует внедрения динамических моделей оценки доверия, способных адаптироваться к меняющимся условиям работы устройств в гетерогенных средах, таких как умные города или промышленные IoT.

Также MFA сталкивается с большими проблемами в области криптографии. Криптографические алгоритмы используются для безопасной связи, согласования ключей, проверки факторов и взаимодействия с DHT / блокчейном. Хотя легковесная криптография стремится минимизировать потребление памяти и энергии, ее эффективность остается под вопросом на низкоуровневых микроконтроллерах.

Легкие примитивы: хэш-функции (например, SHA-256), операции XOR и симметричные шифры (например, AES-128, стандарт NIST ASCON, SPECK) обычно считаются выполнимыми. Моделируемые затраты показывают, что операции занимают от микросекунд до миллисекунд на мощных процессорах, но могут быть значительными на низкоуровневых MCU. В работе [4] было приведено моделируемое время:

– хэш: $T_h \approx 0{,}0026$ мс;

– AES-128 Шифрование / Дешифрование $T_{E/D} \approx 0{,}00325$ мс;

– нечеткое извлечение $T_{FE} \approx 1{,}989$ мс (актуально для биометрии).

Криптография эллиптических кривых (ECC) обеспечивает надежную защиту с меньшими ключами, чем RSA, но требует больших вычислительных затрат. В том же исследовании время умножения точек над ECC (T_{ecm}) оценивалось в 1,989 мс, что значительно выше, чем время хэширования или симметричного шифрования.

Билинейные пары, используемые в некоторых продвинутых схемах [5], еще более требовательны. Пригодность ECC для сильно ограниченных устройств остается спорной, что часто приводит к необходимости перекладывать ее на шлюзы [4].

Для защиты от квантовых компьютеров в будущем требуются алгоритмы PQC, которые часто имеют больший размер ключа/подписи и более высокие вычислительные затраты, чем текущая криптография над ECC.

В работе [6] анализируются требования к устройствам IoT, необходимые для работы алгоритмов PQC.

Главными параметрами этих устройств являются: объем доступной оперативной памяти, объем RAM/флэш-памяти/накопителя и тактовая частота.

Причем объем накопителя не так значителен, как объем RAM, поскольку даже в современных устройствах он обычно не превышает 64 кб.

Если сравнить PQC алгоритмы для создания ЭЦП, то Falcon (0,5 кб) выигрывает у Dilithium (40–70 кб), хотя у Dilithium объем кода гораздо меньше.

В качестве алгоритма инкапсуляции ключей предлагают использовать Kyber или Saber, оба имеют достаточные характеристики для работы с IoT.

Тем не менее, большинство стандартов рассматривают модели, сравнимые с ARM Cortex M4. Большое количество моделей на рынке имеют куда более низкие характеристики.

Другой задачей является обеспечение эффективности MFA. Она зависит от политики, определяющей, какие факторы требуются при тех или иных обстоятельствах (например, аутентификация на основе риска). Децентрализация затрудняет управление политиками:

– как определяются и безопасно распространяются политики MFA среди всех соответствующих субъектов (устройств, валидаторов) в киберфизических системах?

– как последовательно обновляются политики в сети, особенно с учетом проблем с соединением и необходимости консенсуса по изменениям? Задержки в завершении работы блокчейна влияют на скорость распространения политик.

Обеспечение правильного и последовательного применения политик потенциально недоверенными или ограниченными в ресурсах сущностями – сложная задача.

Решение этих взаимосвязанных задач требует целостного подхода. Для этого необходимы достижения в области легковесной и постквантовой криптографии, инновационное использование методов вычислений вне

цепочки. В конечном итоге успешное развертывание MFA в этих средах зависит от нахождения правильного баланса между обеспечением надежной многоуровневой безопасности, поддержанием приемлемой производительности и удобства использования в условиях жестких ограничений на время ожидания и соблюдением жестких ограничений на ресурсы в обширном ландшафте IoT. Для полной реализации потенциала безопасного и эффективного MFA в этих многообещающих, но сложных децентрализованных архитектурах все еще требуются значительные исследования и разработки.

Список использованных источников:

1. Ometov A., Petrov V., Bezzateev S., Andreev S., Koucheryavy Y., Gerla M. Challenges of Multi-Factor Authentication for Securing Advanced IoT Applications // IEEE Network. 2019. Т. 33, № 2. С. 82–88.
2. Muncaster J., Turk M. Continuous multimodal authentication using dynamic Bayesian networks // Proc. 2nd Workshop Multimodal User Authentication, Toulouse, France. 2006. С. 1–8.
3. Phiri J., Zhao T.-J., Zhu C. H., and J. M. Using Artificial Intelligence Techniques to Implement a Multifactor Authentication System // International Journal of Computational Intelligence Systems. 2011. Т. 4, № 4. С. 420–430.
4. Vinoth R., Deborah L., Vijayakumar P., Kumar N. Secure Multi-factor Authenticated Key Agreement Scheme for Industrial IoT // IEEE Internet of Things Journal. 2020. Дек. Т. PP.
5. Nikravan M., Reza A. A Multi-factor User Authentication and Key Agreement Protocol Based on Bilinear Pairing for the Internet of Things // Wirel. Pers. Commun. USA, 2020. Март. Т. 111, № 1. С. 463–494. ISSN 0929-6212.
6. Atkins D. Requirements for post-quantum cryptography on embedded devices in the IoT // Third PQC Standardization Conference. 2021.

Puiko D.D.
North Caucasus Federal University, Stavropol

Scientific supervisor:
Petrenko V.I.
North Caucasus Federal University, Stavropol

PROBLEMS OF MULTIFACTOR AUTHENTICATION IN DECENTRALIZED CYBER-PHYSICAL SYSTEMS

Abstract. Multi-factor authentication (MFA) is of paramount importance for securing cyber-physical systems (CPS), especially in the Internet of Things (IoT) domain characterized by limited device resources and mission-critical operations. Possible mitigation strategies including lightweight cryptography,

off-chain computing, specialized consensus mechanisms, and robust decentralized management protocols are discussed. The challenge is to balance robust security, usability and performance under the severe constraints of these decentralized IoT environments.

Keywords: multi-factor authentication (MFA), Internet of Things (IoT), cyber physical systems (CPS), blockchain.