УДК 621.3.01+621.38

Клімушин Петро Сергійович,
кандидат технічних наук, доцент, доцент кафедри протидії кіберзлочинності Харківського національного університету внутрішніх справ, Харків, Україна, ORCID: https://orcid.org/0000-0002-1020-9399; e-mail: klimushyn@ukr.net
Колісник Тетяна Петрівна,
кандидат педагогічних наук, доцент, доцент кафедри протидії кіберзлочинності Харківського національного університету внутрішніх справ, Харків, Україна, ORCID: https://orcid.org/0000-0002-7442-8136; e-mail: ktp201505@gmail.com
Рог Вікторія Євгенівна,
старший викладач кафедри протидії кіберзлочинності Харківського національного університету внутрішніх справ, Харків, Україна, ORCID:https://orcid.org/0000-0002-7443-5125; e-mail: vitochkarog@gmail.com

АСИМЕТРИЧНА КРИПТОГРАФІЯ: АПАРАТНА ПІДТРИМКА КОДУВАННЯ АСИМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ ВУЗЛІВ ІНТЕРНЕТ РЕЧЕЙ

Клімушин Петро Сергійович,Колісник Тетяна Петрівна,
Рог Вікторія Євгенівна

Харківський національний університет внутрішніх справ, Харків, проспект Льва Ландау,27

Мережа інтернет речей (Internet of Things – IoT) сприяє вирішенню завдань людства в таких сферах, як громадська безпека, управління процесами, сервіс життя людей, медичні послуги, продуктивність і конкурентоспроможність бізнесу.

Безпека функціонування мережі інтернет заснована на ідентифікації та автентифікації її елементів, тобто на визначенні суб’єктів підключення до мережі. Ідентифікація забезпечує надання унікального ім'я суб'єктові – користувачеві, процесу або апаратно-програмному компоненту, а автентифікація пов’язана з діями суб'єктів на другій стороні мережі, за допомогою яких визначається, що суб'єкт першої сторони дійсно той, за кого він себе видає. Тобто синонімом слова "автентифікація" є словосполучення "перевірка дійсності" суб'єкта.

Функціонування мережі інтернет речей засновано на персоналізації суб’єктів з використанням унікальних ідентифікаторів ID, MAC-адресів, ключів і сертифікатів. Використання певної схеми персоналізації має свої

складності в процесі підключення інтернет речей, оскільки її реалізація обумовлює зазначений рівень безпеки та витрат. Тому дана робота присвячена дослідженню технічних рішень з реалізації процедур ідентифікації та автентифікації для забезпечення найвищого рівня безпеки мережі інтернет речей при мінімальних витратах.

Реалізація процедур ідентифікації та автентифікації для забезпечення мережі інтернет речей є актуальним завданням в багатьох середовищах, таких як громадський порядок, енергоефективність, охорона здоров'я, житлові та офісні приміщення, промисловість, транспорт, сільське господарство тощо.

В цих сферах мають значення такі розробки: багатофакторна та безперервна автентифікація IoT [1], розробка протоколів взаємної автентифікації [2], автентифікація IoT на основі блокчейн технології [3, 4] тощо.

Велика увага в мережі IoT приділяється проблемам безпеки збережених, оброблюваних і переданих даних, захисту від клонування кінцевих IoT пристроїв [5, 6], а також захисту від копіювання інтелектуальної власності та цифрового контенту. Критично важливим фактором в захисті інтернет речей стає підтвердження справжності вузла підчас доступу до нього (автентифікування). Тут виникає нова мережна парадигма, яка заснована на взаємодії без участі з людиною, виходячи з таких особливостей побудови IoT: компактність, обмеженість в енергетичних та обчислювальних ресурсах.

Вирішення проблеми забезпечення доступу до об'єктів IoT в умовах нової парадигми можливо при використанні сучасних мікроконтролерів та додаткових криптографічних прискорювачів (криптоакселераторів) з апаратною підтримкою протоколів та криптографічних алгоритмів.

Метою роботи є дослідження способів потенційного застосування криптографічних мікросхем сімейства CryptoAuthentication для проведення безпечної автентентифікації вузлів інтернет речей з використанням процедур асиметричної криптографії.

Слід зазначити, що відповідно до наведеної цілі дана робота є продовженням дослідження [7], яке було присвячено потенційному застосуванню криптографічних мікросхем сімейства CryptoAuthentication з використанням процедур симетричної криптографії, але справжнє дослідження орієнтовано на мікросхеми сімейства CryptoAuthentication асиметричної криптографії.

Забезпечення безпеки мережі IoT включає три основні компоненти (Confidentiality, Integrity, Authenticity – CIA) [5]: справжність (Authenticity) – перевірка дійсності вузла IoT; цілісність (Integrity) – повірка незмінності повідомлення при транспортуванні до місця призначення; конфіденційність (Confidentiality) – доступність даних тільки передбаченим об'єктам або уповноваженим особам.

Мережна безпека забезпечується мережними технологіями на різних рівнях, наборами протоколів, які використовуються в мережі. Слід пам’ятати, що рівень безпеки всієї мережі визначається рівнем безпеки найслабшої ланки [7].

Основними загрозами безпеки вузлів IoT є: порушення захисту на транспортному рівні криптографічних протоколів SSL/TLS; оновлення шкідливим кодом прошивки оригінального програмного забезпечення; не якісне генерування випадкових чисел в криптоалгоритмах; порушення доступу до криптографічних ключів; слабкий захист портів вузлів IoT; фізичне проникнення до вмісту вбудованої пам'яті.

Комплексна безпека вузлів IoT повинна захищати рівномірно від усіх цих загроз. Треба пам’ятати, що наслідки успішної атаки можуть піддати ризику мережу в цілому, тобто все, що підключено до неї.

Вкрай важливо використовувати випробувану методологію – зберігати та використовувати криптографічні ключі протягом усього циклу їх життя в зашифрованому вигляді і в захищеному обладнанні, тобто апаратних модулях безпеки (Hardware Security Module – HSM). Апаратні модулі HSM забезпечують виконання всіх операцій шифрування і розшифрування даних всередині модулю, тобто криптографічні ключі не залишають захищений периметр модулю.

Методом захисту інформації найвищого рівня є застосування криптографічних протоколів з використанням цифрового підпису (ЦП). Вони є основними механізмами при автентифікації, управлінні та сертифікації ключів, а також при безпосередньому захисті інформації в мережі IoT.

При методі асиметричної автентифікації (Asymetric authentication methiod) вся інформація, що вимагає захисту, не розподіляється між суб’єктами взаємодії, а отже потрібен надійний захист на одній зі сторін, що дозволяє економити апаратні та інші ресурси в процесі автентифікації. До того ж використання асиметричних методів забезпечує створення безпечних алгоритмів ЦП, а ЦП є одним із важливих криптографічних перетворень, що застосовуються для забезпечення цілісності, справжності (автентичності), підтвердження авторства, неспростовності повідомлень.

Перевагами апаратних засобів захисту мережі IoT є: апаратний спосіб формування випадкових послідовностей; методологія апаратних модулів безпеки HSM – виконання криптографічних операцій в середовищі захищених криптографічних мікросхем (безпека на кристалі); розмежування та розвантажування функцій центрального процесора вузла IoT за допомогою спеціалізованого криптопроцесора для виконання криптографічних перетворень; гарантування цілісності криптографічних перетворень даних; підвищення швидкості криптографічних перетворень даних.

Ці переваги визначили розвиток апаратних засобів захисту інтернет речей: вбудованих генераторів випадкових послідовностей, криптографічних прискорювачів (криптоакселераторів) та криптографічних модулів у мікропроцесорних комплектах загального призначення.

В роботі дослідженні [8] процедури асиметричної криптографії з застосуванням криптографічних мікросхем сімейства CryptoAuthentication в безпеці інтернет речей, а саме: формування пари (відкритого та закритого) ключів асиметричного шифрування; обчислення цифрового підпису та його перевірки; генерування сеансових (таємних) ключів симетричного шифрування; створення сертифікатів клієнта та підприємства; верифікацію відкритих ключів клієнта і підприємства; верифікацію закритого ключа клієнта та підприємства; захищене завантаження програмного забезпечення, що оновлюється.

Новизною проведеного дослідження є аналіз апаратних засобів підтримки технологій асиметричної криптографії інтернет речей з допомогою криптографічних мікросхем та визначення структурно-функціональних схем для реалізації процедур асиметричної автентифікації вузлів інтернет речей. Відмінними характеристиками наданих схем та процедур асиметричної автентифікації є: забезпечення підвищеного рівня інформаційної безпеки за рахунок захищеного зберігання криптографічних ключів, цифрових підписів, сертифікатів, конфіденційних даних в захищеному від зовнішніх атак апаратному оточенні та не потрібності зберігання закритих ключів клієнтів на стороні хоста. Результатами роботи є процедури та схеми застосування криптомікросхем асиметричної автентифікації для забезпечення захисту вузлів інтернет речей. Аналіз функціонування представлених схем дозволив сформувати наступні висновки. Запропоновані структурно-функціональні схеми для реалізації процедур асиметричної автентифікації вузлів інтернет речей з використанням криптографічних мікросхем надають користувачеві легку можливість реалізувати криптографію без експертних знань в цій галузі. У цих мікросхемах застосовується апаратний блок обчислення і перевірки цифрового підпису ECDSA з перевагами криптографії на еліптичних кривих, як перевірений і надійний алгоритм автентифікації, та блок генерування сеансових ключів симетричного шифрування ECDH. Надані схеми та процедури підтримують три складові інформаційної безпеки, а саме: конфіденційність, цілісність та автентичність даних. Приклади потенційних застосувань наданих схем та процедур можуть бути реалізовані за допомогою будь-якої мікросхеми асиметричної автентифікації, але їх рекомендується застосовувати для генерації сеансових ключів шифрування і там, де для перевірки даних і коду на цілісність і автентичність потрібні цифрові підписи.

Пропозиції подальших досліджень орієнтовані на визначення технологій та ефективних рішень апаратної підтримки криптографії у пристроях-IoT з впровадженням комплексних рішень безпеки, таких як ідентифікація та автентифікація вузлів мережі, симетричне та асиметричне шифрування, криптографічні протоколи, захищене зберігання та генерування ключів, безпечне завантаження і оновлення мікропрограм додатків, підтримка цифрових підписів та сертифікатів, висока криптостійкість та енергоефективність.

Список літератури

1. Falk, R., Fries, S. (2016), “Advanced Device Authentication: Bringing Multi-Factor Authentication and Continuous Authentication to the Internet of Things”, CYBER 2016: The First International Conference on Cyber-Technologies and Cyber-Systems. Germany, P.69–74.
2. Wu, D. J., Taly, A., Shankar, A., Boneh, D. (2017), “Privacy, Discovery, and Authentication for the Internet of Things”, Computer Science. Cryptography and Security, available at: https://arxiv.org/abs/1604.06959 (last accessed 21.05.2021).
3. Yavari, M., Safkhani, M., Kumari, S., Kumar, S., Chen, C.-M. (2020), “An Improved Blockchain-Based Authentication Protocol for IoT Network Management”, Security and Communication Networks, vol. 2020, P. 16. DOI:10.1155/2020/8836214.
4. Tian, Z., Yan, B., Guo, Q., Huang, J., Du, Q. (2020), “Feasibility of Identity Authentication for IoT Based on Blockchain”, Procedia Computer Science, vol. 174, P. 328–332. DOI: 10.1016/j.procs.2020.06.094.
5. CryptoAuthentication™ Family, available at: https://www.microchip.com/en-us/products/security-ics/cryptoauthentication-family (last accessed 21.11.2022).
6. Krivchenko, I. (2015), “Hardware-protected microcircuits of the CryptoAuthentication family: potential applications of ATECCx08A”, Components and technologies. no. 11, P. 57–64.
7. Klimushin, P., Solianyk, T., Kolisnyk, T., Mozhaev, O. (2021), “Potential application of hardware protected symmetric authentication microcircuitsto ensure the securityof internet of things”, Advanced Information Systems, vol.5, No.3, Kharkiv, P. 103 111.
8. Klimushyn, P., Solianyk, T., Mozhaev, O., Nosov, V., Kolisnyk, T., Yanov V. (2021), "Hardware support procedures for asymmetric authentication of the internet of things", Innovative Technologies and Scientific Solutions for Industries, No. 4 (18), P. 31–39. DOI: https://doi.org/10.30837/ITSSI.2021.18.031

Одержано _____.2022