УДК 621.39

МЕТОДИ АУТЕНТИФІКАЦІЇ НА ОСНОВІ ПУБЛІЧНОГО КЛЮЧА В СИСТЕМІ ІНТЕРНЕТУ РЕЧЕЙ

Дуля О.О., Міночкін Д.А.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
Email: sasa97973@gmail.com

METHODS OF THE PUBLIC-KEY BASED AUTHENTICATION IN THE INTERNET OF THINGS

This paper considered a comparative analysis of the methods of the public-key based authentication in the Internet of Things, and the optimal solution based on the comparison is given.

В системі Інтернету Речей (Internet of Things, IoT), аутентифікація - це процес ідентифікації користувачів, пристроїв, додатків і обмеження доступу до авторизованих користувачів і некерованих пристроїв або послуг.

Розглянемо аутентифікацію за допомогою відкритого ключа. У цьому процесі використовуються криптографічні схеми, засновані на імені користувача та паролі, щоб забезпечити надійну безпечну операцію над IoT.

До методів аутентифікації за допомогою відкритого ключа відносяться [1]:

- Симетричне шифрування.
- Шифрування за допомогою публічного ключа, або асиметричне шифрування (Public-key cryptography, PKC).
- Інфраструктура відкритих ключів (Public-key infrastructure, PKI).

Симетричне шифрування використовується для забезпечення конфіденційності повідомлення при його передачі, зберіганні та обробці. Алгоритм симетричного ключа виконує операції шифрування / дешифрування на основі одного ключа, яким користуються дві або більше сторін. Трудність в симетричній криптографії полягає в безпечній доставці ключа від кодувальника до декодера, що може створити ризик безпеки. Той, хто отримує доступ до симетричного ключа, може отримати доступ / змінити / надіслати повідомлення без відома одержувача, що повідомлення було змінено. Для вирішення цих проблем було розроблене шифрування відкритим ключем.

Алгоритми симетричних ключів досить ефективні, але передача ключів є досить складною для кінцевих пристроїв IoT. Розподіл ключів вимагає надійного зв'язку між сервером розподілу ключів та вузлами IoT. PKC ефективним способом забезпечення конфіденційності та аутентифікації. На відміну від симетричного шифрування, PKC базується на математично складній для вирішення задачі [2]. Шифрування відкритим ключем базується на функціях, які легко обчислити, але важко повернути назад без додаткової інформації. У криптосистемі PKC, як правило, у парі ключів, відкритому та приватному ключах, відкритий ключ стає доступним для клієнта, а приватний ключ зберігається в безпечному місці. Захищеність системи безпеки PKC полягає в тому, наскільки важко визначити правильно створений приватний ключ за його відкритим ключем. У цьому випадку довжина закритого ключа важлива для уникнення брут-форс (метод підбору) атак.

RSA (абревіатура від прізвищ Rivest, Shamir та Adleman) - це широко використовуваний алгоритм в шифруванні за допомогою відкритого ключа, в якому складною для обчислення проблемою є пошук простих множників складеного числа [3]. RSA є однією з перших практичних криптосистем з відкритим ключем, яка базується на практичній складності розкладу на добуток двох великих простих чисел. Якщо відкритий ключ достатньо великий, лише той, хто знає прості числа, може здійснити декодування повідомлення. RSA є відносно повільним алгоритмом шифрування, однак він зазвичай використовується для передачі зашифрованих спільних ключів для симетричного шифрування. Оскільки RSA-шифрування є ресурсоємною операцією, в IoT воно використовується в поєднанні з симетричною криптографією. Спільний симетричний ключ зашифрований RSA; безпека шифрування в цілому залежить від довжини ключа. Для RSA потрібна довжина ключа 1024 біта (128 байт), щоб мати еквівалентний рівень безпеки симетричної криптографії довжиною ключа 128 біт (16 байт) [1]. Великий розмір ключа RSA призведе до великих витрат на обчислення.

Еліптична криптографія (Elliptical curve cryptography, ECC) є альтернативою RSA та має кращий захист від атак методом підбору ключів [3]. ECC краще підходить для IoT завдяки значно меншому бітовому розміру

операндів у середовищі, обмеженому ресурсами. ECC - ще один підхід до криптографії з відкритим ключем, який працює на основі еліптичних кривих над скінченними полями. Щоб мати еквівалентний рівень безпеки симетричної криптографії довжиною ключа 128 біт (16 байт) для ключа з ECC шифруванням необхідно 256 біт (32 байт) [1]. Це ефективніше, ніж RSA, і більше підходить для пристроїв з обмеженими ресурсами в Інтернеті речей.

Проблемою використання криптографії з відкритим ключем є впевненість/доказ того, що певний відкритий ключ є справжнім. Він правильний і належить заявленій фізичній або юридичній особі, і не був змінений або замінений зловмисникомм або третьою стороною. Звичайний підхід до вирішення проблеми полягає в використанні PKI, в якому одна або кілька третіх сторін, відомі як центр сертифікації (Certification authority, CA), засвідчують право власності на пари ключів.

PKI - це набір ролей, політик та процедур, необхідних для створення управління, розповсюдження, використання, зберігання та скасування цифрових сертифікатів та управління шифруванням із відкритим ключем. В середовищі IoT загальною проблемою відкритого ключа є вимога аутентифікованого обміну відкритими ключами. PKI складається з компонентів для надійного розповсюдження відкритих ключів. Найважливішим в PKI є довірена третя сторона, яка підписує ідентифікатор сутності своїм приватним ключем.

Висновки. Для системи Інтернету Речей найкращим є метод аутентифікації на основі інфраструктури відкритих ключів (PKI), з використанням ECC шифрування для передачі симетричних ключів.

Література

1. Mousavi, S.K., Ghaffari, A., Besharat, S. et al. Security of internet of things based on cryptographic algorithms: a survey. Wireless Netw 27, 1515–1555 (2021).
2. Mousavi, S.K., Ghaffari, A., Besharat, S. et al. Improving the security of internet of things using cryptographic algorithms: a case of smart irrigation systems. J Ambient Intell Human Comput 12, 2033–2051 (2021).
3. Shancang Li, Li Da Xu Securing the Internet of Things // Syngress, 2007, pp 69-95.