АВТЕНТИФІКАЦІЇ ТА БЕЗПЕКА IOT-ПРИСТРОЇВ У КОНТЕКСТІ АРХІТЕКТУРИ НУЛЬОВОЇ ДОВІРИ

Нєдєльніцев І.В., Антіпов І.Є.
Харківський національний університет радіоелектроніки Харків, Україна

Метою доповіді є аналіз особливостей інтеграції принципів архітектури нульової довіри (ZTA) з пристроями Інтернету речей (IoT) для підвищення рівня їх безпеки без суттєвого зниження зручності та збільшення витрат.

В доповіді наводяться рішення для подолання основних викликів, пов'язаних із впровадженням ZTA в IoT-середовищах, зокрема: використання додаткових факторів автентифікації для зменшення незручностей для користувача, кешування автентифікаційних даних, застосування існуючих бібліотек/технологій для оптимізації витрат на розробку ПЗ, перенесення ресурсомістких обчислювальних операцій у хмарні сервіси задля покращення продуктивності систем та автономності роботи пристроїв.

Надмірна автентифікація в IoT може бути незручною через обмежені інтерфейси пристроїв. Як рішення пропонується використання геолокації, що дозволяє автоматично перевіряти розташування пристроїв і виявляти аномальний доступ [1]. Інший підхід – біометрична автентифікація, яка забезпечує високий рівень безпеки і є зручнішою за паролі [2]. Додатково можна кешувати токени автентифікації для зменшення ручних дій, зберігаючи принципи Zero Trust.

Впровадження складних методів автентифікації збільшує витрати часу і коштів на розробку. Оптимальним є використання готових бібліотек (TLS/SSL, OAuth 2.0, біометрії), що економить ресурси і підвищує надійність [3]. Економічно вигідним рішенням також є використання хмарних сервісів автентифікації від платформ (AWS IoT, Azure IoT), які відповідають сучасним вимогам безпеки.

IoT-пристрої часто обмежені ресурсами і батареєю, що ускладнює постійну автентифікацію. Рішенням є кешування автентифікаційних даних для зменшення навантаження, а також використання легковагих алгоритмів. Інший підхід – винос складних обчислень у хмару, де обчислювальні ресурси необмежені. Пристрій лише надсилає дані і отримує результат, економлячи ресурси та енергію.

Впровадження ZTA в IoT підвищує безпеку, балансуючи між зручністю, витратами на розробку та ресурсними обмеженнями пристроїв. Комбінація підходів дозволяє покращити безпеку IoT без зниження продуктивності чи зручності.

Список літератури

1. Can Zero Trust Work with the IoT? Red River: вебсайт. URL: https://redriver.com/cybersecurity/zero-trust-iot.

2. Importance of Biometric in IoT Application. M2SYS Blog, 2019: вебсайт. URL: https://www.m2sys.com/blog/guest-blog-posts/importance-of-biometric-in-iot-application/.

3. Morrow S. The Dangers of "Rolling Your Own" Encryption. – Infosec Institute, 28.03.2019: вебсайт. URL: https://www.infosecinstitute.com/resources/cryptography/the-dangers-of-rolling-your-own-encryption/.