УДК 004.056

АВТЕНТИФІКАЦІЇ ТА БЕЗПЕКА IOT-ПРИСТРОЇВ У КОНТЕКСТІ АРХІТЕКТУРИ НУЛЬОВОЇ ДОВІРИ

Нєдєльніцев І.В.
e-mail: ivan.niedielnitsev@nure.ua
Харківський національний університет радіоелектроніки, каф. КРІСТЗІ
м. Харків, Україна

Integrating the principles of Zero Trust Architecture (ZTA) with Internet of Things (IoT) devices can greatly improve security, but also poses challenges related to user experience, development costs, and device capabilities. This article highlights the use of geolocation and biometric authentication factors, caching authentication data, leveraging existing security libraries, and moving heavy computing operations to cloud services. Together, these approaches improve ZTA for the IoT without unduly compromising usability or incurring excessive costs.

Ця робота присвячена автентифікації та безпеці IoT-пристроїв у контексті архітектури нульової довіри ZTA. Розглядаються основні виклики, які виникають при впровадженні ZTA в IoT-середовищі, та пропонуються рішення для їх подолання.

1. Зменшення зручності користування

У середовищі IoT надмірно часті запити автентифікації або багатофакторні перевірки можуть бути незручними для користувача. Багато IoT-пристроїв не мають повноцінного інтерфейсу (клавіатури чи екрану) для введення паролів, тому традиційні методи автентифікації знижують зручність. Одним із підходів до вирішення є використання геолокації як додаткового фактору. Геолокаційні технології дозволяють автоматично перевіряти, чи знаходиться пристрій або користувач у очікуваному місці, і таким чином виявляти аномальні спроби доступу [1]. Наприклад, якщо в систему надходить запит на вхід з нетипового місця розташування, архітектура нульової довіри може вимагати додаткової перевірки або відхилити запит. Натомість доступ із дозволеної локації може виконуватися прозоро для користувача, що зменшує кількість ручних дій. Другим важливим методом є біометрична автентифікація – відбитки пальців, розпізнавання обличчя, голосові команди тощо – вже інтегруються у низку IoT-рішень (смарт-замки, голосові помічники тощо). Біометрія забезпечує високий рівень захисту і водночас є зручнішою за паролі, оскільки біометричні ідентифікатори неможливо забути, важко підробити чи передати іншій особі . На відміну від пароля, який може бути вгаданий або викрадений, біометричні характеристики користувача практично неможливо реплікувати або відтворити зі злочинною метою [2]. Використання геолокації та біометрії підвищує довіру до пристрою без постійної участі користувача,

зберігаючи баланс між безпекою і зручністю. Додатково, кешування автентифікаційних даних дозволяє уникнути повторного введення облікових даних і мінімізує переривання роботи, дотримуючись принципів Zero Trust.

2. Здорожчання розробки ПЗ

Впровадження складних схем автентифікації та принципів ZTA вимагає значних ресурсів на розробку програмного забезпечення. Кожен додатковий фактор безпеки, наприклад впровадження модуля для роботи з біометрією або перевірки локації, потребує часу на реалізацію і тестування. Щоб уникнути надмірного збільшення вартості та тривалості розробки, доцільно використовувати існуючі бібліотеки та готові рішення. Замість того щоб створювати власні криптографічні алгоритми чи протоколи автентифікації, розробники можуть інтегрувати перевірені відкриті бібліотеки та фреймворки. Це не лише економить час і кошти, але й підвищує надійність захисту, оскільки добре вивчені стандартні рішення здебільшого краще за саморобні схеми шифрування чи автентифікації [3]. Тому використання поширених і перевірених модулів автентифікації (наприклад, TLS/SSL, OAuth 2.0, бібліотеки роботи з біометричними сенсорами) дозволяє додати рівень нульової довіри без критичного збільшення бюджету проекту. Ще одна економічно вигідна практика – застосування хмарних сервісів автентифікації накшталт AWS IoT, Azure IoT тощо. Залучення таких сервісів іноді дешевше, ніж розробка власного рішення, а постачальники забезпечують відповідність сучасним вимогам безпеки. До того ж, хмарні платформи можуть пропонувати оптимізації, наприклад кешування результатів автентифікації, що знижує операційні витрати [4]. Таким чином, перевикористання наявних рішень і оптимізація викликів допомагають утримати вартість розробки і підтримки системи в допустимих межах, навіть із впровадженням принципів Zero Trust.

3. Обмеження пристроїв

Багато IoT-пристроїв мають обмежені обчислювальні ресурси, невеликий обсяг пам’яті та працюють від батареї. Постійна автентифікація і складні крптоалгоритми перевантажують такі пристрої, спричиняючи затримки та надмірне споживання енергії. Для подолання цієї проблеми використовують два ключові підходи: локальна оптимізація, яка включає кешування автентифікаційних даних і застосування легковагих алгоритмів, і хмарні обчислення. Кешування на рівні пристрою означає, що після первинної автентифікації пристрій тимчасово зберігає, приміром, маркер сеансу, використовуючи його для наступних запитів. Це дозволяє уникнути повторного виконання ресурсомістких криптографічних операцій при кожному з’єднанні. В результаті економиться процесорний час і електроенергія. Інший підхід – винос складних операцій у хмарне середовище. Ідея в тому, щоб максимально переносити важкі обчислення з самого IoT-

пристрою на сервер. Наприклад, замість того щоб мікроконтролер пристрою виконував складні обчислення для біометричної ідентифікації або аналіз поведінкових даних, він може передати ці дані у хмару, де сервер здійснить необхідні розрахунки і надішле результат пристрою. Пристрій все одно повинен автентифікуватися до хмари і шифрувати канал, тому це відповідає концепції Zero Trust, але основне навантаження переміщується із кінцевого вузла[5]. По суті, складні обчислення виконуються в середовищі з «необмеженими» ресурсами, тоді як пристрій надсилає лише необхідні дані та отримує результат, економлячи свій заряд і час. Отже, комбінація кешування та хмарних обчислень дозволяє підтримувати високий рівень безпеки ZTA навіть на малопотужних IoT-пристроях, забезпечуючи прийнятну швидкодію системи.

Впровадження принципів ZTA в IoT-середовищі підвищує захищеність мережі, проте пов'язане з низкою труднощів. Запропоновані підходи дозволяють збалансувати безпеку та ефективність: використання геолокації та біометричних даних мінімізує втручання користувача, кешування автентифікаційної інформації та використання перевірених бібліотек знижують витрати ресурсів і розробки, а перенесення складних обчислень у хмару компенсує обмеження апаратних платформ та збільшують автономність. Комбінування цих методів дає змогу покращити безпеку IoT-пристроїв без суттєвого зниження зручності їх використання та продуктивності. У результаті досягається більш стійка до атак IoT інфраструктура.

Список використаних джерел:

1. Can Zero Trust Work with the IoT? Red River: вебсайт. URL: https://redriver.com/cybersecurity/zero-trust-iot (дата звернення: 01.03.2025).

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/ (дата звернення: 01.03.2025).

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/ (дата звернення: 02.03.2025).

4. AWS IoT Core now supports caching of responses returned by customer's Custom Authorizer Lambdas when using HTTP connections. Amazon Web Services, 08.12.2021: вебсайт. URL: https://aws.amazon.com/about-aws/whats-new/2021/12/aws-iot-core-caching-responses-custom-lambdas/ (дата звернення: 02.03.2025).

5. Efficient Caching for Data-Driven IoT Applications and Fast Content Delivery with Low Latency in ICN, 06.11.2019: вебсайт. URL: https://www.mdpi.com/2076-3417/9/22/4730#:~:text=the%20integration%20of%20mobile%20Internet%2C,the%20offloading%20of%20the%20task (дата звернення: 02.03.2025).