Костюк Кирил Ігорович

Студент ІІІ курсу, спеціальності 123 «Комп’ютерна інженерія»

Київський столичний університет імені Бориса Грінченка, Київ

**РОЗРОБКА ПОЛІТИК БЕЗПЕКИ ДЛЯ ZERO TRUST АРХІТЕКТУРИ В IOT-ІНФРАСТРУКТУРІ**

З розвитком Інтернету речей (IoT) зростає потреба в нових парадигмах забезпечення безпеки, оскільки традиційна периметрова модель вже не може гарантувати належний рівень захисту у відкритому, динамічному та гетерогенному середовищі. Концепція Zero Trust Architecture (ZTA), яка базується на принципі «нікому не довіряй за замовчуванням», стала ключовим напрямом для побудови сучасних моделей захисту [1, c. 2782], особливо в умовах великої кількості недовірених пристроїв, що взаємодіють у розподілених IoT-інфраструктурах.

Основна ідея Zero Trust полягає у постійному контролі доступу, валідації ідентичності, моніторингу контексту сесії та оцінці ризику перед наданням дозволу на взаємодію. У межах цієї статті запропоновано модель формування політик безпеки, що враховує специфіку IoT-середовища, зокрема: обмежені ресурси пристроїв, динамічну змінність контексту, загрози lateral movement, наявність пристроїв з невідомим або скомпрометованим походженням [2, c. 633–635]. Розроблену політику реалізовано на основі моделі контролю доступу ABAC (Attribute-Based Access Control) з урахуванням динамічної оцінки довіри до кожного вузла та поведінкового аналізу трафіку.

Формування політики базується на ідентифікації пристроїв, прив’язці до атрибутів (тип пристрою, рівень ризику, контекст використання, місцезнаходження, роль), визначенні дозволених дій та оцінці поточної поведінки. Формально доступ описується предикатною функцією доступу, де для кожного пристрою ​ та дії виконується перевірка умов , де − множина контекстних факторів. Якщо умова виконується, то дозвіл надається, інакше − доступ блокується [1, c. 2784]. Це забезпечує гнучке управління довірою з можливістю швидкої ревізії політик у випадку змін.

Запропонована архітектура Zero Trust для IoT включає п’ять ключових компонентів: Policy Decision Point (PDP), який ухвалює рішення щодо дозволу; Policy Enforcement Point (PEP) − шлюз або проксі, що виконує рішення; Identity Provider − брокер автентифікації; Telemetry Monitor − збирач поведінкових даних з пристроїв; Trust Engine − механізм обчислення довіри на основі поведінкових моделей і телеметрії [1, c. 2785–2786]. Усі компоненти взаємодіють для забезпечення безперервного контролю та адаптації політики до змін середовища.

Policy Decision Point (PDP) виступає центральним елементом архітектури, який на основі заданих політик та поточного контексту (атрибути пристрою, ресурсу, дії та середовища) ухвалює рішення про доступ. Його реалізація може базуватись на мікросервісах із інтеграцією в системи типу Kubernetes чи Open Policy Agent для масштабування.

Policy Enforcement Point (PEP), зазвичай, реалізується у вигляді шлюзу між IoT-пристроєм та ресурсом. Він виконує рішення PDP, контролює трафік, шифрування, QoS та ізолює пристрій у разі порушень політики, забезпечуючи сегментацію і захист критичних компонентів мережі.

Identity Provider (IDP) здійснює автентифікацію IoT-пристроїв, підтримуючи сертифікати, TPM, Device Fingerprinting, токени (OAuth2, JWT) і протоколи FIDO2/WebAuthn [2, c. 640]. Також IDP формує атрибути для подальшої обробки PDP.

Telemetry Monitor (TM) постійно збирає поведінкові дані (навантаження, API-запити, протоколи), нормалізує їх та передає до Trust Engine (TE), який формує динамічний Trust Score на основі історії активності, шаблонів поведінки та ризиків. TE може застосовувати машинне навчання чи нечітку логіку для класифікації пристроїв за рівнем довіри.

Уся система працює в реальному часі: після підключення нового пристрою IDP ідентифікує його, PDP приймає рішення з урахуванням оцінки TE, а PEP забезпечує виконання. Якщо TM виявляє відхилення у поведінці, Trust Engine знижує рівень довіри, і політика доступу автоматично змінюється – аж до ізоляції пристрою.

Однак запропонований підхід має певні обмеження. По-перше, низькі ресурси IoT-пристроїв унеможливлюють повноцінну локальну перевірку запитів. По-друге, шлюз контролю (PEP) може стати єдиною точкою відмови. По-третє, реалізація системи потребує централізованого журналювання та інтеграції з SIEM-системами для повноцінного виявлення загроз у реальному часі [2, c. 646–647]. Незважаючи на це, запропонована модель демонструє ефективність у зниженні ризику компрометації IoT-інфраструктури.

Таким чином, розроблена політика безпеки для Zero Trust архітектури в IoT-середовищі забезпечує багаторівневий захист за рахунок атрибутивного управління доступом, оцінки довіри, поведінкового аналізу і мікросегментації. Надалі планується дослідити можливості автоматизації оновлення політик на основі машинного навчання, розширити інтеграцію з хмарними SIEM-рішеннями та адаптувати модель до ресурсобідних платформ (наприклад, на базі MicroPython або TinyML).

**Список літератури:**

1. Sarma R., Kumar C., Ahmed Barbhuiya F. ACS-FIT: A Secure and Efficient Access Control Scheme for Fog-enabled IoT // Proceedings of the 2020 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Toronto, ON, Canada, 2020. – P. 2782–2789. – DOI: 10.1109/SMC42975.2020.9283362.
2. Костюк Ю., Хорольська К., Бебешко Б., Довженко Н., Коршун Н., Пазинін А. Інструментальні засоби забезпечення інформаційної безпеки від прихованих загроз в інфраструктурі хмарних обчислень // Кібербезпека: освіта, наука, техніка. – 2025. – Т. 4, № 28. – С. 633–655. – DOI: <https://doi.org/10.28925/2663-4023.2025.28.857>.