УДК 004.056.55:004.738.5:004.42

В. А. Гарнага

ВИКОРИСТАННЯ ПІДХОДІВ ZERO TRUST ARCHITECTURE ПРИ РОЗРОБЦІ МОБІЛЬНИХ ДОДАТКІВ

Вінницький національний технічний університет

Анотація

У доповіді розглядається впровадження принципів Zero Trust Architecture (ZTA) у процес розробки мобільних додатків з метою забезпечення високого рівня кібербезпеки. Аналізуються ключові компоненти ZTA, такі як безперервна автентифікація, принцип найменших привілеїв, мікросегментація та постійний моніторинг, і їхнє застосування в мобільному середовищі. Окрему увагу приділено особливостям реалізації цих принципів на мобільних платформах, а також викликам, що постають перед розробниками у контексті інтеграції ZTA. Наводяться приклади сучасних технічних рішень і рекомендації щодо ефективного використання цього підходу.

Ключові слова: Zero Trust Architecture, мобільні додатки, кібербезпека, автентифікація, мікросегментація, принцип найменших привілеїв.

Abstract

This paper discusses the implementation of Zero Trust Architecture (ZTA) principles in the development of mobile applications to ensure a high level of cybersecurity. It explores key ZTA components such as continuous authentication, least privilege principle, micro-segmentation, and continuous monitoring, and how they are adapted for mobile environments. Special attention is given to the unique challenges of applying ZTA in mobile contexts, as well as practical solutions and best practices for developers.

Keywords: Zero Trust Architecture, mobile applications, cybersecurity, authentication, micro-segmentation, least privilege principle.

Актуальність

Зі зростанням використання мобільних додатків у фінансовій, медичній, освітній та урядовій сферах, питання їх захисту від кіберзагроз стає все більш критичним. Традиційні моделі безпеки, що базуються на припущенні про довіру до внутрішньої мережі, виявляються вразливими до сучасних атак, зокрема фішингу, компрометації облікових записів та атак на ланцюг постачання. У відповідь на ці виклики, модель Zero Trust Architecture пропонує підхід, при якому жоден запит, користувач або пристрій не вважається надійним за замовчуванням. Цей підхід особливо актуальний у сфері мобільних додатків, які часто функціонують за межами корпоративної інфраструктури.

Проаналізуємо принципи Zero Trust Architecture у контексті мобільної безпеки, розглянувши кожен з аспектів окремо.

1. Безперервна автентифікація та авторизація. Один із фундаментальних принципів ZTA полягає в тому, що кожен запит до ресурсу перевіряється заново, навіть якщо користувач вже автентифікований. Це реалізується через багатофакторну автентифікацію (MFA), контекстуальний аналіз (час, місце, тип пристрою) та оцінку ризику. У мобільних додатках це означає, що доступ до даних або функцій додатку може змінюватися залежно від поточних умов. Наприклад, користувач, який зазвичай входить з одного географічного регіону, може бути обмежений при спробі входу з іншого. Також використовуються поведінкові маркери, які дозволяють ідентифікувати аномальні дії у режимі реального часу.

2. Принцип найменших привілеїв (Least Privilege Access). Цей принцип передбачає, що кожному користувачу чи процесу надається лише той рівень доступу, який необхідний для виконання

конкретного завдання. У мобільних додатках це реалізується через модульне управління правами доступу до даних, API та ресурсів пристрою. Наприклад, додаток повинен мати доступ до камери лише в момент, коли користувач виконує дію, яка цього потребує. Використання моделей Role-Based Access Control (RBAC) або Attribute-Based Access Control (ABAC) дозволяє деталізувати політики доступу та динамічно їх оновлювати залежно від умов.

3. Мікросегментація. Мікросегментація передбачає поділ середовища на ізольовані сегменти з незалежним контролем доступу. Для мобільних додатків це означає логічну сегментацію додатку на частини, які взаємодіють лише через чітко регламентовані інтерфейси. Наприклад, автентифікаційний модуль не повинен мати доступ до платіжного модуля без посередництва служби перевірки прав доступу. Це обмежує вплив потенційної компрометації одного компонента на всю систему.

4. Постійний моніторинг і оцінка ризиків. Zero Trust передбачає безперервний моніторинг як мережевої активності, так і поведінки користувачів. У мобільних додатках це може включати інтеграцію із сервісами для поведінкової аналітики, машинного навчання, оцінки ризиків в режимі реального часу. Наприклад, платформа може виявити, що користувач виконує незвичну кількість транзакцій або надто швидко перемикається між екранами — і автоматично призупинити сеанс або вимагати повторну аутентифікацію.

Виклики при впровадженні ZTA у мобільні додатки

Інтеграційна складність. Впровадження Zero Trust вимагає ретельної переробки архітектури існуючих мобільних додатків. Це стосується як програмної логіки, так і взаємодії з серверною частиною.

Вплив на UX. Надмірні заходи безпеки можуть створити незручності для кінцевого користувача, знижуючи задоволення від використання додатку. Тому важливо досягти балансу між зручністю та захищеністю.

Витрати. Побудова Zero Trust-орієнтованої архітектури потребує значних інвестицій у інфраструктуру, навчання персоналу та впровадження нових процесів розробки.

Висновки

Застосування принципів Zero Trust Architecture у процесі розробки мобільних додатків є необхідним кроком для забезпечення високого рівня кібербезпеки в умовах зростаючих загроз. Завдяки гнучкому підходу до управління доступом, постійному моніторингу та принципу недовіри до будь-яких запитів, ZTA дозволяє мінімізувати ризики, пов’язані з витоком даних, несанкціонованим доступом і внутрішніми загрозами. Незважаючи на технічну та організаційну складність впровадження, Zero Trust є перспективною моделлю для побудови безпечних мобільних сервісів нового покоління.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture (NIST Special Publication 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207
2. Microsoft. (2023). Zero Trust Deployment Guide for Mobile Devices. Retrieved from: https://learn.microsoft.com/en-us/security/zero-trust

Гарнага Володимир Анатолійович – кандидат технічних наук, доцент кафедри Захисту інформації, Вінницький національний технічний університет, м. Вінниця, e-mail: garnaga.volodymyr@vntu.edu.ua.
Harnaha Volodymyr – PhD in Technical Sciences, Associate Professor of the Department of Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: garnaga.volodymyr@vntu.edu.ua.