УДК 621.391
О. Колтаков
(Харківський національний університет радіоелектроніки, Україна)

ОГЛЯД ОСНОВНИХ ВРАЗЛИВОСТЕЙ АРХІТЕКТУРИ SDN І МЕТОДІВ ПРОТИДІЇ

UDC 621.391
O. Koltakov

OVERVIEW OF PRINCIPAL VULNERABILITIES IN SDN ARCHITECTURE AND MITIGATION METHODS

Програмно-конфігуровані мережі (Software-Defined Network, SDN) представляють підхід до побудови мереж, в якому функції управління відокремлено від площини даних і реалізовано програмно, що забезпечує гнучкість, масштабованість і спрощене адміністрування. Водночас архітектура SDN, що включає площину даних, площину управління та площину застосунків [1], має низку вразливостей, пов'язаних із централізованою природою площини управління та використанням стандартизованих інтерфейсів взаємодії, які можуть слугувати потенційними точками атаки. Забезпечення комплексної безпеки вимагає усунення ризиків на кожному з архітектурних рівнів і впровадженні відповідних політик безпеки. В даній роботі проведено огляд основних вразливостей архітектури SDN і методів протидії.

DDoS-атаки на контролер SDN є одними з найкритичніших, оскільки можуть спричиняти переповнення таблиці потоків (flow table) SDN-комутатора, виснаження обчислювальних ресурсів та втрату керованості мережею. Відповідно у роботі [1] рекомендовано фреймворк FloodDefender, спрямований на виявлення та зниження впливу таких атак шляхом аналізу трафіку та фільтрації зловмисних пакетів. Крім того, трафік площини даних в SDN є вразливим до перехоплення й модифікації, що створює додаткові ризики компрометації вузлів або перехоплення управління ними. Водночас застосування стійких механізмів шифрування дозволяє усунути дану вразливість. Також канал взаємодії між контролером мережі та застосунками може бути вразливим через недостатньо надійні механізми автентифікації та авторизації. Одним із підходів до запобігання такого несанкціонованого доступу є використання спеціалізованих модулів автентифікації, зокрема рішення IZTSDN, запропонованого в роботі [2].

Таким чином, у роботі проаналізовано основні вразливості архітектури SDN та характерні загрози. Виявлено, що більшість типів атак відомі з практики традиційних телекомунікаційних мереж (ТКМ), проте особливості SDN можуть підвищувати чутливість ТКМ до окремих атак. Це підкреслює необхідність поєднання класичних підходів до забезпечення безпеки з багаторівневими механізмами захисту, адаптованими до специфіки програмно-конфігурованих мереж.

Література

1. Anand, N., Saifulla, M.A., Ponnuru, R.B., Alavalapati, G.R., Patan, R. and Gandomi, A.H., 2024. Securing software defined networks: A comprehensive analysis of approaches, applications, and future strategies against DoS attacks. IEEE Access, Vol. 13, pp. 64473-64515, 2025. DOI: https://doi.org/10.1109/ACCESS.2024.3520478.
2. Guo, X., Xian, H., Feng, T., Jiang, Y., Zhang, D., Fang, J., 2023. An intelligent zero trust secure framework for software defined networking. PeerJ Computer Science, 9, e1674. DOI: https://doi.org/10.7717/peerj-cs.1674.