УДК 004.056.5
Д. Марчук; В. Тимощук
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

АРХІТЕКТУРА БЕЗПЕКИ ЯДРА 5G НА ОСНОВІ ВІРТУАЛІЗОВАНИХ МЕРЕЖЕВИХ ФУНКЦІЙ ТА УЗГОДЖЕНИХ ПОЛІТИК

UDC 004.056.5
D. Marchuk; V. Tymoshchuk

SECURITY ARCHITECTURE FOR THE 5G CORE BASED ON VIRTUALIZED NETWORK FUNCTIONS AND HARMONIZED POLICIES

Розвиток мобільних мереж п’ятого покоління із широким використанням NFV, SDN, сервісно-орієнтованої архітектури (SBA), network slicing та MEC радикально ускладнює завдання побудови цілісної системи кібербезпеки ядра 5G Core [1]. Інтенсивне впровадження віртуалізованих мережевих функцій, динамічне масштабування сервісів та поява великої кількості взаємодіючих доменів управління призводять до того, що традиційні засоби захисту та статичні політики доступу виявляються недостатніми. Додаткові ризики створюють компроміси на користь продуктивності, зокрема захист цілісності у площині користувача, як опція, кешування станів у stateful-фаєрволах та активне використання проксі та сервісної сітки (service mesh). Усе це суттєво ускладнює своєчасне виявлення загроз і точну локалізацію атак у межах 5G Core.

У роботі представлено політико-керовану архітектуру безпеки 5G Core зі замкненими контурами управління, що забезпечує узгоджену синхронізацію політик MANO/ZSM [2] та мінімізує побічний вплив контрзаходів на легітимні сервіси. Архітектура базується на ієрархії доменного та локальних оркестраторів безпеки з інтегрованими компонентами Policy Decision Point та Policy Enforcement Point, які використовують двоступеневу модель політик HSPL/MSPL і модуль Policy Conflict Detector для автоматизованої перевірки клієнтських політик відносно глобальних правил оператора. Особливу увагу приділено двом критичним класам вразливостей: атакам на таблиці станів stateful-фаєрволів для протоколів без стану з’єднання та маніпуляціям DHCP/RA-повідомленнями, що транспортуються через площину користувача без гарантованого захисту цілісності.

Для захисту від атак на таблиці станів запропоновано механізм таргетованого керування записами станів, який дозволяє локалізувати шкідливу активність без глобального скидання таблиці. Для протидії маніпуляціям DHCP/RA-повідомленнями запропоновано механізм автентифікації службових полів з використанням криптографічних перевірок, що забезпечують підтвердження походження повідомлень без необхідності повного увімкнення захисту цілісності для всього користувацького трафіку. Запропоновані підходи апробовано на експериментальному стенді з використанням Open5GS, контейнеризації CNF в Kubernetes та інтеграцією Suricata, Kafka й Drools, де продемонстровано скорочення часу реагування на атаки та зменшення кількості побічних відмов сервісу в сегментованих 5G-середовищах.

Література

1. 5G Core. Supermicro. URL: https://www.supermicro.com/en/glossary/5g-core (date of access: 01.12.2025)
2. . IETF | Internet Engineering Task Force. URL: https://www.ietf.org/proceedings/88/slides/slides-88-opsawg-6.pdf (дата звернення: 01.12.2025).
3. Open5GS. GitHub. URL: https://github.com/open5gs (date of access: 01.12.2025).