УДК 621.391

ВДОСКОНАЛЕНА МОДЕЛЬ БЕЗПЕКИ 5G

Кормульов О. С.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: steallex214@gmail.com

ENHANCED 5G SECURITY MODEL

This article introduces an improved 5G security model to help secure networks against all kinds of attacks and threats. Its main elements and characteristics are described in detail. The security features of 5G networks, its dependence on various factors have been investigated as well.

Висока швидкість 5G відкриває величезне поле можливостей: нові види послуг, сервісів та цілі бізнес-моделі, які здавалися неможливими в мережах минулих поколінь. До переваг 5G в порівнянні з мережами минулих поколінь можна віднести можливість підключення великої кількості пристроїв, високу енергоефективність, високу мобільність користувачів; в декілька разів зросла пропускна здатність, яка дозволяє забезпечити більшу доступність широкосмугового мобільного зв'язку.

Але з новими перевагами та плюсами, новими системами з’являться і нові вразливі місця. Для захисту 5G від вдосконалених і складних видів загроз потрібна розвинена модель безпеки (яка зображена на рис. 1.), яка пропонує глибокий захист не тільки від існуючих, але і від еволюціонуючих та нових видів загроз, а також загроз нульового дня. Це вимагатиме чітко визначеної стратегії безпеки та плану захисту різних компонентів для мережі 5G, включаючи кінцеві пристрої та кінцевих користувачів. Ефективна стратегія безпеки може бути розроблена на основі телеметричних даних, отриманих за допомогою добре розробленої системи спостереження. Необхідно визначити процеси та інструменти для участі у виявленні атак та нападів на систему, блокувати їх та розвивати систему захисту мережі.

Забезпечення належного рівня безпеки є обов'язковим для видів загроз які постійно змінюються та атак на системи безпеки 5G мереж. Для посилення безпеки та захисту даних користувачів, модель безпеки має відповідати наступним вимогам та параметрам:

1) *Конфіденційність*: в моделі безпеки 5G конфіденційність даних є однією з основних вимог безпеки; властивість, яка може захистити передачу даних від розголошення її стороннім особам та від пасивних атак (тобто, прослуховування та підслуховування). Враховуючи архітектури 4G-LTE та 5G, будь-які дані користувача повинні бути конфіденційними та захищеними від несанкціонованих користувачів. Стандартні алгоритми шифрування даних широко прийняті для реалізації конфіденційності даних у мережевих додатках 5G (наприклад, мережах транспортних засобів, моніторингу стану здоров'я тощо). Симетричні криптосистеми можуть бути використані для шифрування та дешифрування даних 5G одним і тим же приватним криптографічним

ключем. Вони обмінюються між комунікаційними об'єктами (наприклад, відправником та одержувачем).

Рис. 1. Посилена модель безпеки 5G розпізнавання загроз.

Симетричні криптосистеми можуть бути використані для шифрування та дешифрування даних 5G одним і тим же приватним криптографічним ключем. Вони обмінюються між комунікаційними об'єктами (наприклад, відправником та одержувачем).

2) *Цілісність*: запобігання втручанню та втраті інформації під час її переміщення з однієї точки в іншу. Цілісність даних в 5G NR захищена аналогічно 4G. У 5G NR цілісність захищена бездротовим трафіком даних на рівні протоколу конвергенції пакетних даних (PDCP). У 4G LTE захищеність цілісності забезпечується лише для шару (рівня) без доступу (NAS) та шару доступу (AS). Однак однією з головних відмін у захисті цілісності 5G є те, що 5G NR також забезпечує захист цілісності площини користувача. Це важливо, оскільки в 4G такої функції не було. Ця нова функція корисна для невеликих передач даних, особливо для обмежених пристроїв IoT. Більше того, механізм автентифікації 5G 5G-AKA використовує захищену телесигналізацію. Це гарантує, що жодна сторона, яка не має права, не може змінювати та отримувати доступ до інформації, яка передається в ефірі.

3) *Доступність*: у області 5G доступність мереж - це забезпечення доступності мережевих ресурсів тоді, коли вони будуть потрібні законним користувачам, оскільки доступність впливає на репутацію постачальника послуг. Іншими словами, доступність забезпечує високу ймовірність ефективності мережевої інфраструктури. Вона також вимірює стійкість мережі проти активних атак, наприклад, DoS-атак. Атака DoS може погіршити продуктивність мережі. Однак за допомогою надширокосмугового мобільного зв’язку (eMBB) та надвисокого надійного MachineType-зв'язку (uMTC)

доступність мережі може бути досягнута як мінімум на 95% та 99,99% відповідно, при їх застосуванні в 5G мережі.

4) *Централізована політика безпеки*: архітектури безпеки 3GPP 4G не можуть безпосередньо застосовуватися для використання в мережах 5G, оскільки вони присвячені традиційній моделі довіри оператор-абонент. Тому для підтримки нових інновацій (таких як NFV та SDN) існує потреба у централізованій системі управління політикою безпеки, яка забезпечує зручність доступу користувачів до додатків та ресурсів. Для цього можна використовувати структуру управління безпекою на основі політик (policy-based) для підтримки централізованого управління безпекою для 5G. Цей метод полягає в тому, що він використовується для прийняття рішень з проблемами безпеки на основі політик, встановленими адміністратором мережі, або оператором. Крім того, оператори можуть включити Security-as-a-Service (SaaS) як потенційне рішення проблем з безпекою для ряду клієнтів

5) *Видимість*: дозволяє ефективно вирішити основні проблеми мережі для забезпечення безпечного середовища. Мережам 5G необхідно використовувати комплексні стратегії наскрізного (end-to-end) захисту які повинні охоплювати всі рівні мережі. Для реалізації такого всебічного механізму безпеки 5G-оператори повинні мати повну видимість, перевірку та контроль над усіма рівнями мережі. Технології 5G повинні бути інтегровані з відкритими API для управління політикою безпеки.

Таким чином, мережа 5G може мати послідовну політику безпеки як програмного, так і апаратного забезпечення в мережі. Покращена видимість всієї мережі та політик безпеки допоможуть реалізувати нові посилені механізми безпеки, що підходить для нових послуг 5G. Більше того, покращення видимості дозволяє запобігти загрозам, що керують даними, знаходити та ізолювати заражені пристрої до того, як вони вчинили атаку на мережу.

У роботі представлено вдосконалену модель безпеки 5G, яка допомагає захистити мережі від будь-яких видів атак та загроз. Детально описано та зображено її основні елементи, вимоги, параметри та характеристики. Також досліджено особливості безпеки мереж 5G, її залежність від різноманітних факторів. Проблеми безпеки та конфіденційності зв’язку будуть більш помітні, коли до 5G мереж буде підключено більше користувачів. Врахування цих можливих загроз від початкових етапів проектування до розгортання самих мереж 5G зведе до мінімуму ймовірність можливих помилок безпеки та конфіденційності.

Література

1. A Comprehensive Guide to 5G Security / Madhusanka Liyanage; Ijaz Ahmad; Ahmed Bux Abro; Andrei Gurtov; Mika Ylianttila, 1st Edition вид. Helsinki, Finland: Kindle Edition, 2017.
2. Ijaz Ahmad. Tanesh Kumar, Madhusanka Liyanage, Jude Okwuibe, Mika Ylianttila, Andrei Gurtov 5G security: Analysis of threats and solutions // 2017 IEEE Conference on Standards for Communications and Networking (CSCN). Helsinki, Finland: 2017.
3. 5G Security White Paper // Huawei. 2019.