УДК 621.391

МЕТОДИ ЗАБЕЗПЕЧЕННЯ ЗАДАНИХ ПОКАЗНИКІВ БЕЗПЕКИ В 5G МЕРЕЖАХ

Правило В.В., Кормульов О.С.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: v.v.pravylo@ukr.net, steallex214@gmail.com

Methods of ensuring specified security indicators in 5G networks

In this paper, we consider several possible threats in 5G networks and also discover a methods for solving them.

З швидким розвитком мобільних мереж п'ятого покоління постає питання в забезпеченні безпеки в цих мережах. Незважаючи на те, що в стандарти 5G включені вбудовані функції безпеки, самої по собі мережевої інфраструктури недостатньо для вирішення всіх проблем, пов'язаних з безпекою. На відміну від мереж попередніх поколінь, 5G підтримує більше видів послуг та має більш широкий спектр задач. Такі технології, як пристрої, підключені до Інтернету речей (IoT), доповненої реальності (AR), віртуальної реальності (VR) та інші, вимагають швидкої, надійної та обширної мережі, щоб не відставати від темпів розвитку. Нові підприємства та нові технології, що працюють в епоху 5G, зіткнуться з новими проблемами безпеки та конфіденційності.

Майбутні мережі зв'язку 5G не тільки успадкують уразливості мереж четвертого покоління, а й можуть обзавестися новими недоліками безпеки. Поряд з високою швидкістю (в 10-1000 разів більшою ніж у 4G), низьким енергоспоживанням і мінімальними затримками сигналу, очікується активне використання в мережах 5G технологій віртуалізації мережевих функцій (Network Function Virtualization). Заміна апаратних елементів програмними має багато позитивних ефектів, проте потенційно зробить стільникові мережі ще більш уразливими для атак зловмисників.

Проведемо аналіз вразливих місць в 5G за допомогою простого прикладу – модельна непублічна 5G-мережа (Non-Public Network, NPN) підключену до зовнішнього світу через канали зв'язку загального користування (Рис. 1).

Саме такі мережі будуть використовуватися в найближчому майбутньому. Потенційне середовище розгортання мереж такої конфігурації - «розумні» підприємства, «розумні» міста, офіси великих компаній і інші аналогічні локації з високим ступенем контрольованості.

Як показано на Рис 1., NPN має фундаментальну вразливість у своїй конструкції. Система безпеки, яка працює у внутрішніх мережах NPN, захищає об'єкт і його приватне хмарне сховище, система безпеки вбудована в систему - свою внутрішню інфраструктуру. Трафік між NPN і зовнішніми мережами вважається безпечним, оскільки виходить з захищених систем, але фактично його нічого не захищає. На цій ділянці відсутній видимий IT-

моніторинг безпеки. Багато роумінгових-, міжміських-, радіо- та інших видів атак, можуть спричинити компрометацію інформації, а отже, і самої мережі 5G.

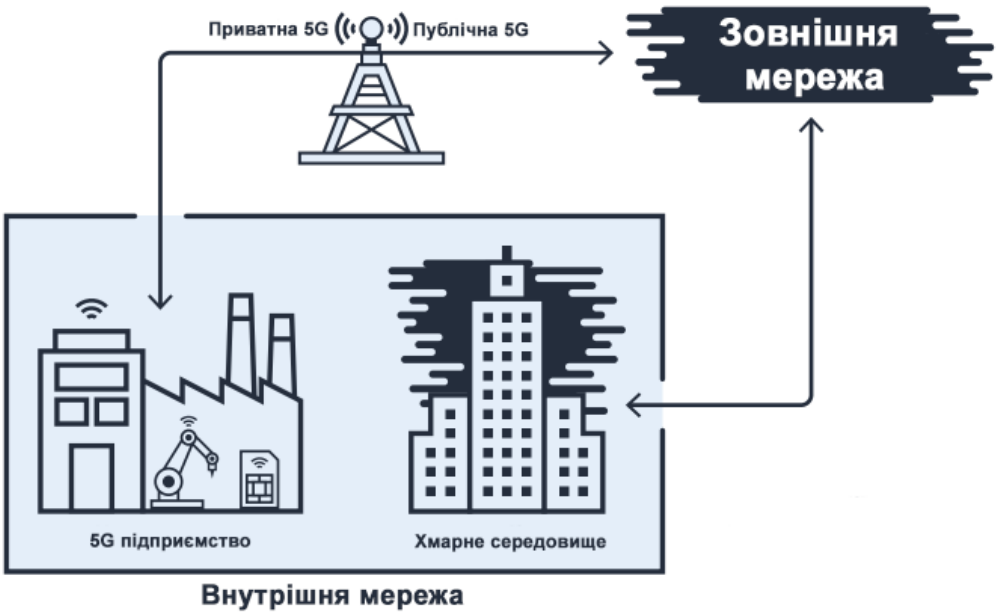

Рис. 1. Непублічна 5G мережа. Закрита мережа підприємства підключена до глобальної 5G-мережі через публічні канали.

Виникає декілька можливих сценаріїв кібератак на мережі 5G, які експлуатують:

- Уразливості SIM-карт
- Уразливості мережі
- Уразливості систем ідентифікації

При атаках апаратного рівня може використовуватися метод віддалених маніпуляцій з SIM-картою (SIMjacking) в роумінгу (тобто при роботі поза "домашньої" мережі). Наприклад, модифікація її налаштувань таким чином, щоб пристрій користувача підключався не до публічної мережі, а до мережі, якою керують кіберзлочинці. Завдяки змінам в налаштуваннях SIM-карти хакери зможуть здійснювати прослуховування розмов користувача, впроваджувати шкідливі програми та заважати алгоритмам машинного навчання.

При атаках на дані і саму мережу, зламана SIM-карта використовується для того, щоб погіршити продуктивність самого пристрою і мережі, до якої він підключений або навіть змінити базові налаштування цієї мережі. Атаки salami і low-and-slow дозволять з часом створити в інфраструктурі мережі "сліпі плями", які хакери зможуть використовувати для більш масштабних кібератак.

В атаках із застосуванням телекомунікаційних каналів і посвідчень повноважень доступу, зловмисники користуються тим, що існує певна невідповідність між способами обробки посвідчень ідентифікації в IT-системах і цих каналах. Велика частина посвідчень і облікових даних в телекомунікаційних каналах прив'язана до SIM-картки і обробляється на

апаратному рівні, а в IT-інфраструктурі - на рівні ПО. Відповідно, після крадіжки особистості користувача за допомогою злому карти, хакери отримують доступ і до IT-систем, які налаштовані так, щоб автоматично "довіряти" пристрою з цієї SIM-картою. В результаті цього, вони можуть використовувати цю вразливість для обходу систем захисту від шахрайських дій, змін функцій мережі і навіть змін кінцевих продуктів, якщо мова йде про виробництво.

Уразливості NPN-мережі 5G - наслідок розрізненості процедур безпеки на комунікаційному рівні, рівні SIM-карт і пристроїв, а також на рівні роумінгової взаємодії мереж. Щоб вирішити цю проблему, необхідно відповідно до принципу нульової довіри (Zero-Trust Architecture, ZTA) забезпечити перевірку справжності пристроїв, які підключаються до мережі, на кожному етапі, запровадивши федеративну модель ідентифікації та управління доступом (Federated Identity and Access Management, FIdAM).

Принцип ZTA полягає в підтримці безпеки навіть коли пристрій непідконтрольно, коли він рухається або перебуває за межами периметра мережі. Федеративна модель ідентифікації - це підхід до безпеки 5G, який забезпечує єдину узгоджену архітектуру для перевірки автентичності, прав доступу, цілісності даних і інших компонентів і технологій в мережах 5G.

Такий підхід виключає можливість впровадити в мережу «роумінгову» вишку і перенаправити на неї захоплені SIM-карти. IT-системи зможуть повноцінно виявити підключення сторонніх пристроїв і блокувати паразитний трафік, що створює статистичний шум.

Для захисту SIM-карти від модифікації необхідно впровадити в неї додаткові засоби перевірки цілісності, наприклад, реалізовані у вигляді SIM-додатку на базі блокчейна. Додаток може використовуватися для аутентифікації пристроїв і користувачів, а також для перевірки цілісності прошивки і налаштувань SIM-карти як в роумінгу, так і при роботі в домашній мережі.

Отже, рішення виявлених проблем безпеки 5G можна представити у вигляді об'єднання трьох підходів:

- впровадження федеративної моделі ідентифікації та управління доступом, яка забезпечить цілісність даних в мережі;
- забезпечення повної видимості загроз шляхом реалізації розподіленого реєстру для перевірки легітимності і цілісності SIM-карт;
- формування розподіленої системи безпеки, що вирішує питання взаємодії з пристроями в роумінгу.

Література

1.https://www.ec-rs.ru/blog/novosti/positive-technologies-zapuskaet-servis-po-otsenke-zashchishchennosti-setey-4g-i-5g/

2. https://habr.com/ru/company/trendmicro/blog/486262/

3. Craig Gibson - Securing 5G Through Cyber-Telecom Identity Federation https://documents.trendmicro.com/assets/white_papers/wp-securing-5g-through-cyber-telecom-identity-federation.pdf

4. http://www.dailycomm.ru/m/49398/