УДК 621.382

АНАЛІЗ ПОТЕНЦІЙНИХ ВРАЗЛИВОСТЕЙ ТА ЗАГРОЗ В 5G

Правило В.В.
Навчально-науковий Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: v.v.pravylo@ukr.net

ANALYSIS OF POTENTIAL VULNERABILITIES AND THREATS IN 5G

Vulnerabilities of 5G networks and critical infrastructure are considered. The criticality classification of 5G infrastructure assets is given.

З поточних опублікованих стандартів і досліджень, проведених в співтоваристві 5G, були виявлені деякі помітні вразливості. Ці уразливості можуть бути усунені в майбутніх випусках стандартів, і очікується, що деякі з них будуть усунені після завершення розробки стандартів 5G. Вразливості розбиті на три розділи: конфіденційність, цілісність і доступність (CIA). Тріада CIA, як відомо, є наріжним каменем політики безпеки і визначає найбільш важливі компоненти безпеки. Цілком імовірно, що деякі з них будуть розглянуті в майбутньому, однак деякі висновки буде важко пом'якшити, і станом на випуск 15 3GPP вони як і раніше вразливі [1].

Конфіденційність. Конфіденційність − це принцип, згідно з яким конфіденційні дані не будуть передані сторонам, які не мають потреби або повноважень на доступ. У разі стільникового зв’язку це може означати текстові повідомлення, телефонні дзвінки та інтернет-трафік. У просторі 5G з IoT це може означати медичні пристрої, які збирають дані для практикуючих лікарів, або обладнання для управління будівлею, яке дозволяє входити в територію. Важливо, щоб ці дані були захищені від загроз, щоб запобігти ненавмисному витоку персональних даних або даних безпеки [2].

Цілісність. Цілісність − це принцип підтримки точності та узгодженості даних від кінцевої точки до точки, і це важливо для бездротового зв’язку, щоб запобігти маніпуляціям даними через фактори навколишнього середовища або зловмисних суб’єктів. Специфікації бездротового зв’язку часто включають методи повторної передачі даних, щоб подолати розриви або перешкоди та продовжити з’єднання. Важливо, щоб ці дані були перевірені, щоб вони точно збіглися з тими, які надіслав пристрій. Наслідки для прийнятих змінених даних можуть бути як збій у телефонній розмові, так і катастрофічними, як електростанції, які отримують неправильні контрольні коди.

Доступність. Доступність − це третя частина тріади CIA. Цей принцип вимагає, щоб усі інформаційні системи були функціональними та завжди доступними. Це важлива мета, тому що без доступності ніщо інше не має значення. Якщо система недоступна, вона нікому не корисна. Коли ви маєте справу зі стільниковими мережами, область, яка не поширюється, може мати серйозні наслідки. В нинішній час більшість користувачів не мають

стаціонарних телефонів, а громадських телефонів дуже мало. Коли йдеться про безпеку життєдіяльності, а комунікація має вирішальне значення, система, яка забезпечує комунікації, є життєво важливою.

Розвиток розуміння критичної інфраструктури. При виборі критичності телекомунікаційних елементів, які повинні піддаватися особливій перевірці, основну увагу слід приділяти критичній інфраструктурі, яка визначається як:

– Державні мережі та центри обробки даних.

– Інфраструктура, яка використовується постачальниками основних продуктів і послуг: енергетика, продовольство, сировина, залізниці, аеропорти, телекомунікації, банки, інтернет-біржі, водоканали, лікарні.

– Інфраструктура критично важлива для високоцінних підприємств або має ключове стратегічне значення для економіки країни.

Необхідно розуміти, що критичність мереж і конкретних мережевих елементів повинна оцінюватися на основі (потенційно порушених) додатків, підтримуваних цими мережами. Навіть короткочасний збій в підключенні в обмеженій географічній зоні або вплив на вимоги до затримки для критично важливої послуги може призвести до смертельних наслідків. Таким чином, безперешкодний доступ до підключення стає таким же важливим, як і доступ до електрики.

Мережі 5G будуть засновані на хмарі, тобто їх інфраструктура буде складатися з взаємопов'язаних центрів обробки даних, або "хмар". Вони забезпечують середовище віртуалізації, в якому мережеві функції виконуються як віртуальні мережеві функції в загальній інфраструктурі, що надає віртуалізовані обчислювальні, мережеві та запам'ятовуючі ресурси.

Центри обробки даних будуть з'єднані між собою транспортними мережами, що складаються з вузлів транспортної мережі (наприклад, оптичних комутаторів) і фактичних ліній зв'язку (наприклад, оптоволоконних мереж). Транспортні мережі також забезпечать взаємозв'язок між центрами обробки даних, що належать до різних мереж мобільного зв'язку, що полегшить роумінг і зв'язок між абонентами різних мереж.

Мобільний доступ (RAN) складається з антен, радіочастотного та широкосмугового обладнання. У 5G RAN може бути реалізований в різних топологіях, починаючи від "класичних" розподілених мереж, заснованих на специфічній функції фізичної мережі HW (PNF), до віртуалізованих архітектур (vRAN /VNF), заснованих на великій кількості Edge Cloud (граничних хмар). Edge Cloud не буде виділена для RAN, але також буде містити частину Ядра, в основному шлюзи, і додатки для реалізації варіантів використання з низькою затримкою, підтримуваних 5G. Ось чому різниця між мобільним доступом і ядром стає все більш розмитою.

Хоча пристрої, що використовують мережу, зазвичай не є активами операторів мобільного зв'язку, вони все одно можуть містити, відповідно до специфікацій 3GPP, захищене обладнання, зазвичай відоме як "SIM-карта", але в специфікаціях зване UICC (Universal Integrated Circuit Card). UICC знаходиться під контролем оператора мережі і містить дані і програмне забезпечення, зване додатком USIM (Universal Subscriber Identity Module).

Додаток USIM на UICC має важливе значення для безпечного зв'язку між пристроєм і мережею і може розглядатися як частина активів операторів мобільного зв'язку. Для пристроїв Інтернету речей UICC може бути вбудований, і тільки його частина USIM знаходиться під контролем оператора.

Таблиця 1. Класифікація критичності інфраструктурних активів 5G.

Функція 5G / мережевий елемент	*Класифікація*	*Коментар*
Центри обробки даних	Критична	- Центри обробки даних розміщують: критично важливі функції мережі 5G, конфіденційні мережеві і призначені для користувача дані, а також інтерфейси до інших мереж. - ближче до границі (DC) ризик може зменшитися, оскільки вплив успішних атак носить регіональний характер.
Транспортні мережі (вузли і лінії зв'язку, наприклад, оптичні комутатори і волокна; Комутатори SDN)	Висока	- фізичний вплив, можливе порушення роботи мережі, - загроза прослуховування може бути зменшена за допомогою шифрування, - резервування дозволяє долати атаки на окремі транспортні вузли та канали
Об'єкти IPX	Висока	- подібно до транспортних мереж, трафік може бути захищений за допомогою механізмів, зазначених у 3GPP, або механізмів, визначених іншими організаціями, такими як GSMA.
Невіртуалізовані базові станції	Середня	- Атаки зазвичай мають локальний вплив, можливо надмірне покриття з інших базових станцій, конфіденційні дані захищені в захищеному середовищі базової станції; однак впровадження DoS-атаки в ядро також представляє ризик
Антена	Низька	- Низький рівень впливу; тільки локалізовані DoS-атаки
UICC/USIM	Низька	- висока апаратна безпека, дуже локальний вплив при зломі або клонуванні USIM

Класифікація критичності заснована на географічному охопленні/кількості абонентів, які постраждали в разі збою [3]. Однак фактичний рівень ризику залежить від програм, які можуть бути скомпрометовані.

Література

1. R. Piqueras Jover and V. Marojevic. “Security and Protocol Exploit Analysis of the 5G Specifications”. In: IEEE Access 7 (2019), 24956–24963. ISSN: 2169-3536. doi: 10.1109/ACCESS.2019.2899254.
2. Kim Zetter et al. Florida Cops’ Secret Weapon: Warrantless Cellphone Tracking. 2014. URL: https://www.wired.com/2014/03/stingray/.
3. Nokia. 5G Security Risks and Mitigation Measures. URL: https://www.nokia.com/sites/default/files/2021-05/Whitepaper-5G-security-Nokia-STC-March-31-2021.pdf.