УДК 004.056
DOI: 10.31673/2409-7292.2023.010008

Захаржевський А. Г., Герасимчук О. С.

КОМПЛЕКСНА АРХІТЕКТУРА БЕЗПЕКИ У МЕРЕЖАХ 5G НА ОСНОВІ ПОБУДОВИ ДОМЕНІВ ДОВІРИ

У статті розглянуто ключові підходи до побудови системи безпеки у мережах 5G. Визначено, що архітектура безпеки у мережах 5G базується на використанні технологій 3G та 4G у поєднанні з новими протоколами та функціями. Показано, що перелік уразливостей мереж 5G розширюється через децентралізацію, що створює можливість для атаки на обчислювальні ресурси локальних пристроїв, які апріорі захищені слабше, ніж центральні вузли ядра мережі. Досліджено концепцію побудови доменів довіри, які дозволяють будувати комплексний захист з урахуванням можливості здійснення атак на різних рівнях.

Ключові слова: мережа 5G, домен, довіра, атака, кібербезпека.

Вступ

Мережі 5-го покоління є еволюцією мереж 4-го покоління LTE. Нова технологія пропонує високі швидкості передачі даних (понад 1 Гбіт/с), затримку менше 1 мс і можливість одночасного підключення близько 1 мільйона пристроїв у радіусі 1 км^2. Такі високі вимоги, які ставляться до мереж п'ятого покоління, позначилися і принципах їх організації. При цьому, найбільших змін зазнали технології радіодоступу. Для мереж 5-го покоління була розроблена нова RAT (Radio Access Technology) – 5G New Radio. Що стосується ядра мережі, воно зазнало не таких значних змін. У зв'язку з цим архітектура безпеки 5G-мереж була розроблена з акцентом на використання відповідних технологій, прийнятих у стандарті 4G LTE.

Постановка проблеми

Варто відзначити, що переосмислення таких відомих загроз, як атаки на радіоінтерфейси та рівень сигналізації (signalling plane), DDOS-атаки, Man-in-the-Middle атаки та ін, спонукало операторів зв'язку розробити нові стандарти та інтегрувати абсолютно нові механізми безпеки у мережі 5-го покоління.

Одним з ключових принципів побудови мереж 5G є децентралізація, яка має на увазі розміщення множини локальних баз даних та центрів їх обробки на периферії мережі. Це дозволяє мінімізувати затримки при M2M-комунікаціях і розвантажити ядро мережі через обслуговування величезної кількості пристроїв IoT. Таким чином, межа мережі розширюється, дозволяючи створювати локальні центри комунікації та надавати хмарні послуги без ризику критичних затримок або відмови в обслуговуванні. Змінений підхід до організації мереж та обслуговування клієнтів відкриває перед зловмисниками нові можливості для атак як на конфіденційну інформацію користувачів, так і на самі компоненти мережі з метою викликати відмову в обслуговуванні або захопити обчислювальні ресурси оператора. Таким чином, оцінка потенційних уразливостей та побудова комплексної архітектури безпеки для мереж 5G є актуальним науковим та практичним завданням.

Аналіз публікацій

Питанням захисту мереж 5G присвячено значну кількість публікацій. Так, у [1] представлена архітектура безпеки мереж 5G і зазначено, що вона базується на архітектурі безпеки 3G/4G, але розширює та вдосконалює їх, щоб охопити нове середовище 5G.

У [2] представлено ландшафт загроз у мережах 5G, а також обговорюється доцільність і архітектура різних моделей на основі машинного навчання для протидії цим загрозам. Крім того, представлено архітектуру для автоматизованого аналізу загроз із використанням кооперативного та скоординованого машинного навчання для захисту активів та інфраструктури 5G.

У [3] наведено аспекти безпеки системи 5G, визначені Проектом Партнерства Третього Покоління (3GPP), підкреслюючи її відмінності від системи 4G (LTE). Найважливішими вдосконаленнями безпеки 5G є первинна автентифікація без доступу, встановлення та

керування ключами безпеки, безпека для мобільності, безпека архітектури на основі послуг, безпека між мережами, конфіденційність і безпека для послуг, що надаються через 5G із вторинною автентифікацією.

В той же час, наразі відсутні публікації, які б дозволили розглянути безпеку мереж 5G комплексно, у взаємодії між кінцевими користувачами та ядром мережі з урахуванням відмінностей мереж 5-го покоління від їх попередників.

Метою цієї роботи є формування архітектури безпеки у мережах 5G на основі побудови доменів довіри.

Основні уразливості мереж 5-го покоління

Розширені можливості для атаки. При побудові телекомунікаційних мереж 3-го та 4-го поколінь оператори зв'язку зазвичай обмежувалися роботою з одним або кількома вендорами, які одразу постачали комплекс апаратного та програмного забезпечення. При цьому не було необхідності замінювати чи доповнювати пропрієтарне ПЗ. Сучасні тенденції спрямовані на віртуалізацію мереж, мультивендорний підхід до їх побудови та різноманітність ПЗ, зокрема технології SDN (Software Defined Network) і NFV (Network Functions Virtualization), що призводить до включення величезної кількості ПЗ, побудованого на базі відкритих вихідних кодів. Це дає зловмисникам можливість краще вивчити мережу оператора та виявити більшу кількість уразливостей.

Велика кількість IoT-пристроїв. На теперішній час близько 60% пристроїв, підключених до 5G-мереж, становлять IoT-пристрої. Це означає, що більшість хостів мають обмежені криптографічні можливості і, відповідно, є вразливими до атак.

Обмежені криптографічні можливості IoT-пристроїв. Через підключення великої кількості IoT-пристроїв, які, внаслідок своїх невеликих розмірів і малого енергоспоживання, мають дуже обмежені обчислювальні ресурси, мережі 5G стають вразливими до атак, спрямованих на перехоплення управління з подальшою маніпуляцією такими пристроями.

Децентралізація та розширення меж мережі. Периферійні пристрої, що відіграють роль локальних ядер мережі, здійснюють маршрутизацію трафіку користувача, обробку запитів, а також локальне кешування і зберігання даних. Таким чином, межі мереж 5-го покоління розширюються, окрім ядра, на периферію, у тому числі на локальні бази даних та радіоінтерфейси 5G-NR (5G New Radio). Це створює можливість для атаки на обчислювальні ресурси локальних пристроїв, які апріорі захищені слабше, ніж центральні вузли ядра мережі, з метою викликати відмову в обслуговуванні.

На даний час ETSI і 3GPP опублікували вже більше 10 стандартів, що стосуються різних аспектів безпеки 5G мереж. Переважна більшість механізмів, описаних там, орієнтована на захист від уразливостей (в т.ч. і описаних вище). Одним із основних є стандарт TS 23.501 версії 15.6.0, що описує архітектуру безпеки мереж 5-го покоління.

Архітектура мереж 5G

Для початку розглянемо ключові принципи архітектури 5G-мереж, які дозволять повною мірою розкрити зміст та зони відповідальності кожного програмного модуля та кожної функції безпеки 5G.

1. Поділ мережних вузлів на елементи, що забезпечують роботу протоколів користувача (UP – User Plane) та елементи, що забезпечують роботу протоколів управління (CP – Control Plane), що підвищує гнучкість в частині масштабування та розгортання мережі.
2. Підтримка механізму network slicing, ґрунтуючись на послугах, що надаються конкретним групам кінцевих користувачів.
3. Реалізація мережевих елементів як віртуальних мережевих функцій.
4. Підтримка одночасного доступу до централізованих та локальних служб, тобто реалізація концепцій хмарних (fog computing) та граничних (edge computing) обчислень.
5. Реалізація конвергентної архітектури, що поєднує різні типи мереж доступу – 3GPP 5G New Radio та non-3GPP (Wi-Fi тощо) з єдиним ядром мережі.

6. Підтримка єдиних алгоритмів та процедур аутентифікації незалежно від типу доступу.
7. Підтримка мережевих функцій без збереження стану (stateless), в яких обчислюваний ресурс відокремлений від сховища ресурсів.
8. Підтримка роумінгу з маршрутизацією трафіку як через домашню мережу (home-routed roaming), так і з локальним підключенням (local breakout) у гостьовій мережі.
9. Сервіс-орієнтована та інтерфейсна взаємодія між мережевими функціями.

Концепція безпеки мереж 5-го покоління включає елементи: 1) аутентифікацію користувача з боку мережі; 2) аутентифікацію мережі з боку користувача; 3) узгодження криптографічних ключів між мережею та користувачем; 4) шифрування та контроль цілісності сигнального трафіку; 5) шифрування та контроль цілісності користувальницького трафіку; 6) захист користувача; 7) захист інтерфейсів між різними елементами мережі; 8) ізоляцію різних шарів механізму network slicing; 9) аутентифікацію користувача та захист трафіку на рівні кінцевих сервісів (IMS, IoT та ін.).

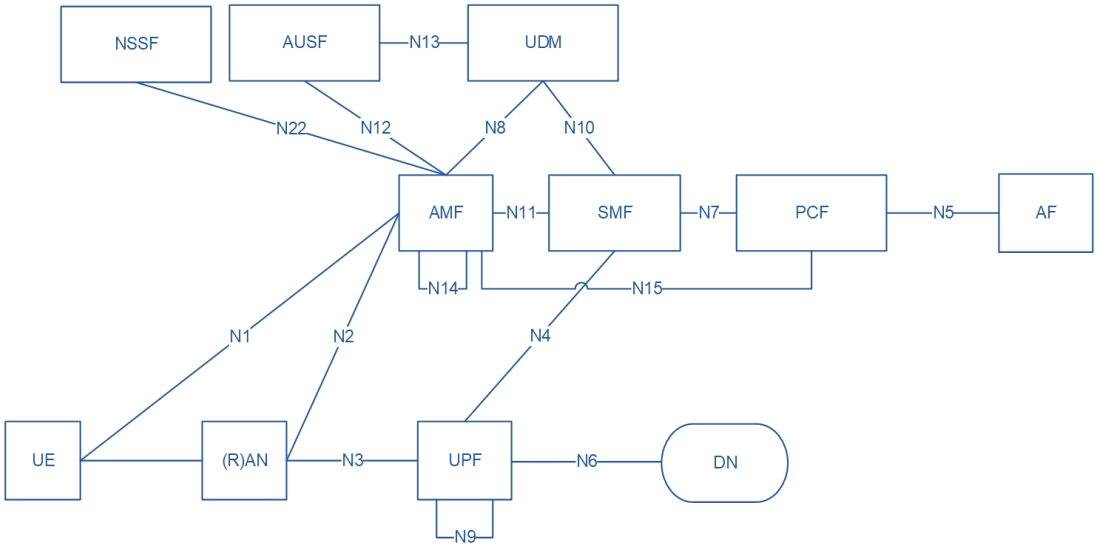

Рис. 1. Основні програмні модулі та мережеві функції безпеки 5G [4]

Таблиця 1

Відповідність програмних модулів функціям безпеки у мережах 5G

Програмний модуль	**Функції безпеки**
AMF (Access and Mobility Management Function – функція управління доступом та мобільністю)	- організація інтерфейсів керування; - організація обміну сигнальним трафіком RRC/NAS, шифрування та захист даних; - управління реєстрацією та з'єднанням обладнання в мережі; - управління доступністю обладнання користувача в мережі в стані CM-IDLE; - управління мобільністю обладнання в мережі в стані CM-CONNECTED; - надсилання коротких повідомлень між власним обладнанням та SMF; - управління службами геолокації; - виділення ідентифікатора потоку EPS для взаємодії з EPS.
ARPF (Authentication Credential Repository and Processing Function – функція сховища та обробки облікових даних аутентифікації)	- зберігання персональних секретних ключів (KI) та криптографічних алгоритмів; - генерація векторів аутентифікації відповідно до 5G-AKA або EAP-AKA. *Розміщується у захищеному від зовнішніх фізичних впливів ЦОД домашнього оператора зв'язку та, як правило, інтегрується з UDM.*
AUSF (Authentication Server Function – функція сервера аутентифікації)	- відіграє роль сервера аутентифікації, що приймає і обробляє запити від SEAF і перенаправляє їх в ARPF.

Програмний модуль	Функції безпеки
NEF (Network Exposure Function – функція мережної експозиції)	- організація безпечної взаємодії зовнішніх платформ та програм з ядром мережі; - керування параметрами QoS та правилами тарифікації для конкретних користувачів.
PCF (Policy Control Function – функція контролю політик)	- формування та призначення користувачам політик обслуговування, включаючи параметри QoS та правила тарифікації.
SCMF (Security Context Management Function – функція управління контекстом безпеки)	- керування життєвим циклом контексту безпеки 5G.
SEAF (Security Anchor Function – якірна функція безпеки)	- спільно з AUSF забезпечує аутентифікацію користувачів при їх реєстрації в мережі з будь-якою технологією доступу.
SIDF (Subscription Identifier De-concealing Function – функція вилучення ідентифікатора користувача)	- вилучення постійного ідентифікатора підписки абонента (SUPI) з прихованого ідентифікатора (SUCI), отриманого в рамках запиту процедури аутентифікації Auth Info Req.
SMF (Session Management Function – функція управління сесіями)	- управління сесіями зв'язку, підтримка тунелю між мережею доступу та UPF; - розподіл та керування IP-адресами користувача обладнання; - вибір шлюзу UPF; - організація взаємодії з PCF; - управління застосуванням QoS; - динамічне настроювання обладнання за допомогою DHCPv4 та DHCPv6; - контроль збору тарифікаційних даних та організація взаємодії із системою білінгу; - безшовність надання послуг (SSC – Session and Service Continuity); - взаємодія з гостьовими мережами в рамках роумінгу.
SPCF (Security Policy Control Function – функція управління політикою безпеки)	- узгодження та застосування політик безпеки щодо конкретних користувачів: вибір AUSF, вибір алгоритму аутентифікації, шифрування даних і контролю цілісності, визначення довжини і життєвого циклу ключів.
UDM (Unified Data Management – уніфікована база даних)	- керування даними профілів користувачів; - управління SUPI; - генерація облікових даних аутентифікації 3GPP AKA; - авторизація доступу на основі даних профілю (наприклад, обмеження роумінгу); - управління реєстрацією користувача, тобто зберігання обслуговуючої AMF; - підтримка безшовності обслуговування та сеансу зв'язку, тобто зберігання SMF; - управління доставкою SMS.
UDR (Unified Data Repository – сховище уніфікованих даних)	- зберігання різних даних користувача (база даних усіх абонентів мережі).
UDSF (Unstructured Data Storage Function – функція зберігання неструктурованих даних)	- зберігання модулями AMF поточних контекстів зареєстрованих користувачів для забезпечення безшовності та безперервності абонентських сесій як за планового виведення з сервісу одного з AMF, так і при виникненні аварійної ситуації.
UPF (User Plane Function – функція площини користувача)	- взаємодія із зовнішніми мережами, у тому числі до глобального Інтернету; - маршрутизація пакетів користувачів; - маркування пакетів відповідно до політик QoS; - діагностика пакетів користувачів (виявлення програм на основі сигнатур); - надання звітів про використання трафіку. UPF є якорною точкою для підтримки мобільності як усередині однієї, так і між різними технологіями радіодоступу.

Поєднання UDR та UDSF на одній фізичній платформі є типовою реалізацією даних мережевих функцій.

Основні вимоги безпеки до мереж зв'язку 5G

Аутентифікація користувача: Обслуговуюча мережа 5G повинна аутентифікувати SUPI користувача в процесі 5G AKA між користувачем і мережею.

Аутентифікація обслуговуючої мережі: Користувач повинен аутентифікувати ідентифікатор обслуговуючої мережі 5G, причому аутентифікація забезпечується через успішне використання ключів, отриманих в результаті процедури 5G AKA.

Авторизація користувача: Мережа, що обслуговує, повинна авторизувати користувача за профілем користувача, отриманим з мережі домашнього оператора зв'язку.

Авторизація мережі мережі домашнього оператора: Користувачеві має бути надано підтвердження того, що він підключений до мережі, яка авторизована мережею домашнього оператора для надання послуг.

Авторизація мережі доступу мережею домашнього оператора: Користувачеві має бути надано підтвердження того, що він підключений до мережі доступу, яка авторизована мережею домашнього оператора для надання послуг.

Неавтентифіковані аварійні сервіси: Щоб відповідати нормативним вимогам у деяких регіонах, 5G-мережі мають надавати можливість неавтентифікованого доступу для аварійних сервісів.

Ядро мережі та мережа радіодоступу: У ядрі мережі 5G та мережі радіодоступу 5G має підтримуватися використання алгоритмів шифрування та збереження цілісності з довжиною ключа 128 біт для забезпечення безпеки AS та NAS. Мережні інтерфейси повинні підтримувати 256-бітові ключі шифрування.

Основні вимоги безпеки до обладнання користувача

Користувальне обладнання повинно підтримувати:

шифрування, захист цілісності та захист від атак повторного відтворення даних;

механізми шифрування та захисту цілісності даних за вказівкою, отриманою від мережі радіодоступу;

шифрування, захист цілісності та захист від атак повторного відтворення сигнального трафіку RRC та NAS;

криптоалгоритми: NEA0, NIA0, 128-NEA1, 128-NIA1, 128-NEA2, 128-NIA2 (може підтримувати також 128-NEA3, 128-NIA3);

криптоалгоритми: 128-EEA1, 128-EEA2, 128-EIA1, 128-EIA2 у випадку, якщо воно підтримує підключення до мережі радіодоступу E-UTRA;

захист конфіденційності даних, що передаються між користувальницьким обладнанням і мережею радіодоступу (опціонально);

захист конфіденційності сигнального трафіку RRC та NAS (опціонально).

Постійний ключ користувача повинен бути захищений і зберігатися в добре захищених компонентах обладнання. Постійний ідентифікатор передплати абонента не повинен передаватися у відкритому вигляді через мережу радіодоступу за винятком інформації, необхідної для коректної маршрутизації (наприклад, MCC та MNC). Відкритий ключ мережі домашнього оператора, ідентифікатор цього ключа, ідентифікатор схеми захисту та маршрутизаційний ідентифікатор повинні зберігатися у USIM.

Основні вимоги безпеки до мережних функцій 5G

AMF має підтримувати первинну автентифікацію за допомогою SUCI.

SEAF має підтримувати первинну автентифікацію за допомогою SUCI.

UDM та ARPF повинні зберігати постійний ключ користувача та забезпечувати його захист від крадіжки.

AUSF повинна надавати SUPI локальній обслуговуючій мережі тільки у разі успішної первинної аутентифікації з використанням SUCI.

NEF не повинна пересилати приховану інформацію про ядр мережі за межі домену безпеки оператора.

Реалізація процедур безпеки 5G на основі доменів довіри

У мережах 5-го покоління довіра до елементів мережі будується за кільцевим принципом і знижується при віддаленні елементів від ядра мережі. Ця концепція впливає на рішення, реалізовані в архітектурі безпеки 5G. Таким чином, можна говорити про модель довіри 5G-мереж, яка визначає поведінку механізмів безпеки мережі.

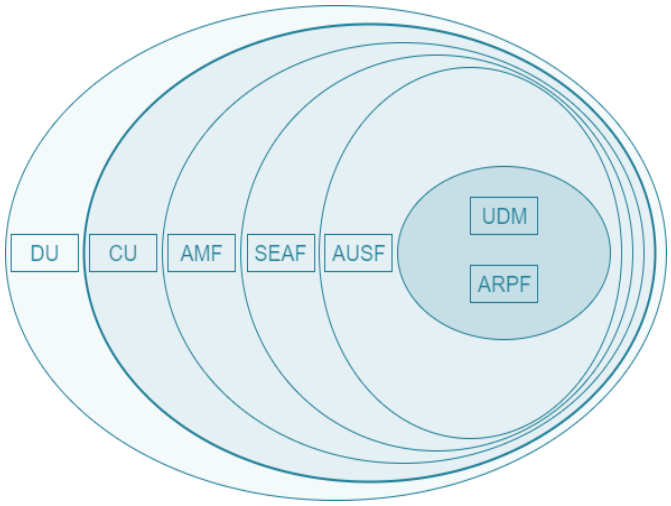

Рис. 2. Загальна модель доменів довіри для мереж 5G [3, 4]

З боку користувача домен довіри утворюють UICC та USIM.

На боці мережі домен довіри має складнішу структуру. Мережа радіодоступу поділяється на дві складові – DU (Distributed Units – розподілені одиниці мережі) і CU (Central Units – центральні одиниці мережі). Разом вони формують gNB – радіоінтерфейс базової станції мережі 5G. DU не мають безпосереднього доступу до даних користувача, оскільки можуть бути розгорнуті в сегментах незахищеної інфраструктури. CU повинні бути розгорнуті в захищених сегментах мережі, оскільки відповідають за термінацію трафіку механізмів безпеки AS.

У ядрі мережі розташовується AMF, що термінує трафік механізмів безпеки NAS. У поточній специфікації 3GPP 5G Phase 1 описано суміщення AMF з функцією безпеки SEAF, що містить кореневий ключ (також відомий як «якірний ключ») відвідуваної мережі. AUSF відповідає за зберігання ключа, отриманого після успішної автентифікації. Він потрібний для повторного використання у випадках з одночасним підключенням користувача до кількох мереж радіодоступу. ARPF зберігає облікові дані користувачів та є аналогом USIM у абонентів. UDR і UDM зберігають інформацію користувача, яку використовують для визначення логіки генерації облікових даних, ідентифікаторів користувачів, забезпечення безперервності сесії та ін.

Неавтономна безпека NR

Першим кроком, стандартизованим 3GPP до повного покриття 5G, був Non-Standalone NR, також відомий як E-UTRA-NR Dual Connectivity (EN-DC) або архітектура «Варіант 3» [5]. Ключовою особливістю Non-Standalone є можливість використовувати існуючу інфраструктуру LTE та EPC, що робить радіотехнологію на основі 5G доступною без заміни мережі. EN-DC використовує LTE як головну технологію радіодоступу, тоді як нова технологія радіодоступу (тобто NR) служить вторинною технологією радіодоступу з обладнанням користувача (UE), підключеним до обох радіостанцій. За винятком узгодження можливостей, процедури безпеки для EN-DC в основному відповідають специфікаціям безпеки подвійного підключення для 4G.

Головний eNB (MeNB) перевіряє, чи має UE можливості 5G NR для доступу до вторинного gNB (SgNB), тобто базової станції 5G, і права доступу до SgNB. Перевірка можливостей і прав доступу гарантує сумісність стандарту, оскільки UE з різними можливостями, включаючи можливості безпеки, можуть приєднуватися до мережі.

MeNB отримує та надсилає ключ, який буде використовуватися SgNB для безпечного зв'язку через NR; UE також отримує той самий ключ. На відміну від подвійного підключення в мережах 4G, повідомленнями керування радіоресурсами (RRC) можна обмінюватися між UE та SgNB, таким чином ключі, які використовуються для захисту цілісності та конфіденційності повідомлень RRC, а також даних User Plane (UP) виводяться. Хоча захист цілісності даних UP підтримується в мережі 5G, він не використовуватиметься у випадку EN-DC. Використання захисту конфіденційності є необов'язковим як для UP, так і для RRC.

Варіанти моделі доменів довіри

Модель довіри на стороні мережі для випадків роумінгу та без роумінгу показано на рис. 3 і 4 відповідно, де показано шари довіри на кількох рівнях.

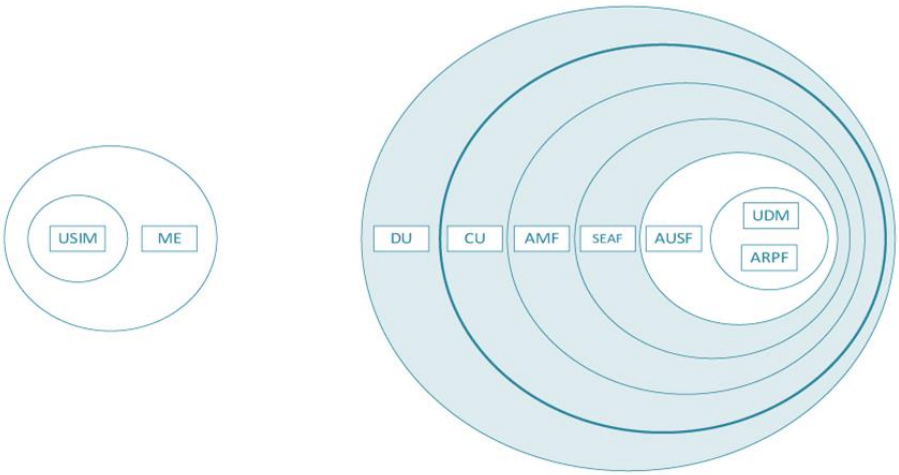

Рис. 3. Модель доменів довіри для нероумінгового сценарію [3]

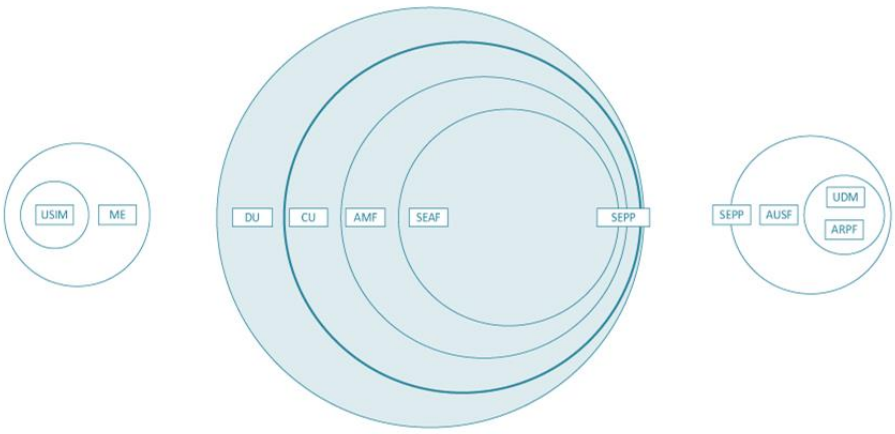

Рис. 4. Модель доменів довіри для роумінгового сценарію [3]

У базовій мережі функція керування доступом (AMF) служить кінцевою точкою для безпеки Non-Access Stratum (NAS). Наразі, тобто в специфікації 3GPP 5G Phase 1 [6], AMF

поєднується з функцією прив'язки безпеки (SEAF), яка зберігає кореневий ключ (відомий як прив'язний ключ) для відвіданої мережі. Така архітектура безпеки дозволяє відокремити прив'язку безпеки від функції мобільності, що може бути можливим у майбутній еволюції архітектури системи.

Функція AUthentication (AUSF) зберігає ключ для повторного використання, отриманий після автентифікації, у разі одночасної реєстрації UE в різних мережевих технологіях доступу, тобто мережах доступу 3GPP і мережах доступу без 3GPP, таких як бездротова локальна мережа IEEE 802.11 (WLAN). Репозиторій облікових даних автентифікації та функція обробки (ARPF) зберігає облікові дані автентифікації. Це відображається USIM на стороні клієнта, тобто на стороні UE. Інформація про абонента зберігається в Єдиному сховищі даних (UDR). Уніфіковане керування даними (UDM) використовує дані підписки, що зберігаються в UDR, і реалізує логіку програми для виконання різних функцій, таких як генерація облікових даних для автентифікації, ідентифікація користувача, обслуговування та безперервність сеансу тощо. Через безпроводовий інтерфейс розглядаються як активні, так і пасивні атаки як на процеси керування, так і на користувача.

В архітектурі роумінгу домашня та відвідувана мережі з'єднані через SEPP (SEcurity Protection Proxy) для рівня керування міжмережевим з'єднанням. Це покращення зроблено в 5G через значну кількість атак, наприклад, атаки на крадіжку ключів і перемаршрутизацію в SS7 [7], а також підробку адреси джерела в сигнальних повідомленнях у DIAMETER [8], які використовували довірені характер міжмережевого з'єднання [9].

Висновок

Незважаючи на те, що архітектура безпеки 5G базується на використанні існуючих технологій, перед нею ставляться нові завдання. Величезна кількість IoT-пристроїв, розширені межі мережі та елементи децентралізованої архітектури – ось лише деякі з ключових принципів стандарту 5G, що дають волю фантазії кіберзлочинців. Побудова системи безпеки для мереж 5G на основі доменів довіри зменшує ризики, пов'язані з децентралізацією та розширенням меж мережі.

Перелік посилань

1. Arfaoui, Ghada & Bisson, Pascal & Blom, Rolf & Borgaonkar, Ravishankar & Englund, Hakan & Félix, Edith & Klaedtke, Felix & Nakarmi, Prajwol & Naslund, Mats & O'Hanlon, Piers & Papay, Juri & Suomalainen, Jani & Surridge, Mike & Wary, jean-philippe & Zahariev, Alexander. (2018). A Security Architecture for 5G Networks. IEEE Access. PP. 1-1. 10.1109/ACCESS.2018.2827419.
2. Amir Afaq, Noman Haider, Muhammad Zeeshan Baig, Komal S. Khan, Muhammad Imran, Imran Razzak, Machine learning for 5G security: Architecture, recent advances, and challenges, Ad Hoc Networks, Volume 123, 2021, 102667, ISSN 1570-8705, https://doi.org/10.1016/j.adhoc.2021.102667.
3. Anand R. Prasad, Sivabalan Arumugam, Sheeba B., and Alf Zugenmaier. 3GPP 5G Security. Journal of ICT, Vol. 6 1&2, 137–158. River Publishers doi: 10.13052/jicts2245-800X.619
4. Введение в архитектуру безопасности 5G: NFV, ключи и 2 аутентификации. https://habr.com/ru/post/481446/
5. 3GPP TS 33.401, "Technical Specification Group Services and System Aspects: 3GPP System Architecture Evolution (SAE) Security architecture".
6. 3GPP TS 33.501, "Security architecture and procedures for 5G system".
7. Tobias Engel. (December 2014). "SS7: Locate. Track. Manipulate" (Chaos Computer Club Berlin)
8. GSMA RIFS: "Diameter Roaming Security - Proposed Permanent Reference Document".
9. 3GPP TR 33.899, "Study on the security aspects of the next generation system", Rel. 14, v 1.3.0, Aug. 2017.

Надійшла: 02.01.2023 Рецензент: д.т.н., професор Кожухівський А.Д.